I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes

IRA S. RUBINSTEIN*

Abstract: According to its many critics, privacy self-regulation is a failure. It suffers from an overall lack of transparency, weak or incomplete realization of the Fair Information Practice Principles, inadequate incentives to ensure wide-scale industry participation, and ineffective compliance and enforcement mechanisms. Rather than attacking or defending self-regulation, this Article explores co-regulatory approaches in which government plays a role in setting requirements for industry guidelines and imposing sanctions for non-compliance. It examines innovative policy tools such as regulatory covenants and develops a normative framework for evaluating self-regulatory mechanisms. It then considers four case studies, including a voluntary code governing online behavioral advertising practices, a government-negotiated program enabling data flows between Europe and the U.S., a statutory safe harbor program designed to protect children's privacy, and a variety of privacy covenants. This Article argues that while statutory safe harbors have many strengths and privacy covenants offer the promise of achieving even better results, both would benefit from being redesigned. Finally, it offers specific policy recommendations: (1) to the FTC on how it might begin to use the covenanting approach to experiment with

* Adjunct Professor of Law and Senior Fellow, Information Law Institute, New York University School of Law. For their extensive comments on an earlier draft of this paper, I am especially grateful to Dennis Hirsch, Chris Hoofnagle, and Ron Lee. I also benefited from the comments and suggestions of Malcolm Crompton, Charles Curran, Amy Mudge, Peter Schuck, and Lisa Sotto, and the participants in the Workshop on Federal Privacy Legislation, New York University School of Law, October 2, 2009.

innovative technologies and address hard problems such as online behavioral advertising; and (2) to Congress on how best to structure new safe harbor programs as an essential component of omnibus consumer privacy legislation. All of these approaches to regulatory innovation move beyond purely voluntary codes in favor of co-regulatory solutions.

INTRODUCTION

Privacy policy in the U.S. has long relied on a combination of sectoral law, market forces, and self-regulation. Over the years, the Department of Commerce (DOC) and the Federal Trade Commission (FTC) have expressly favored a self-regulatory approach. They argue that self-regulation can protect privacy in a more flexible and cost-effective manner than direct regulation without impeding the rapid pace of innovation in Internet-related businesses.

Privacy self-regulation generally involves a trade association or group of firms establishing substantive rules concerning the collection, use, and transfer of personal information, and procedures for applying these rules to member firms.[1] But, to its many critics, self-regulation in the form of such voluntary codes has been a failure.[2] It suffers from an overall lack of accountability and transparency, incomplete realization of the Fair Information Practice Principles (FIPPs),[3] free rider issues, and weak oversight and enforcement.

---

[1] *See* Peter P. Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*, *in* PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (U.S. Dep't of Commerce ed., 1997), *available at* http://www.ntia.doc.gov/reports/privacy/selfreg1.htm.

[2] *See infra* Part II.

[3] FIPPs are the basis for modern privacy regulation, but have been challenged in recent years by privacy scholars and technologists. *See infra* note 202 and accompanying text. There are different formulations of FIPPs, which vary as to both the number of principles and their substantive content. The original formulation dates from the early 1970s. *See* U.S. DEP'T OF HEALTH & HUMAN SERVS., RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (1973), *available at* http://aspe.hhs.gov/datcncl/1973privacy/tocprefacemembers.htm. A recent U.S. government formulation includes eight principles (transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, and accountability and auditing). *See* U.S. DEP'T OF HOMELAND SEC., PRIVACY POLICY GUIDANCE MEMORANDUM: THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE DEP'T OF HOMELAND SECURITY (2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

Indeed, privacy self-regulation has been derided as chimera whose real purpose is to avoid government regulation.[4] More often than not, these same critics call upon Congress to intervene in the online marketplace by enacting comprehensive privacy legislation. Under this enforcement model of regulation, Congress would define substantive privacy requirements for commercial firms based on FIPPs and authorize agency regulation as supplemented over time by court decisions interpreting their requirements. The legislation would also spell out which agencies have enforcement authority, what remedies are available, and whether individuals have a private right of action to recover damages for any injuries they might suffer when a firm violates the law.[5]

The opposing sides in the privacy debate tend to view self-regulation and government regulation as if they were mutually exclusive options from which policy makers had to choose either one or the other. But this is short-sighted. Modern regulatory theory treats self-regulation as a "highly malleable term which may encompass a wide variety of instruments."[6] Thus, it is better to think of voluntary codes and direct government regulation as opposing ends of a regulatory continuum, with most self-regulatory schemes falling somewhere in the middle. Rather than attacking or defending familiar forms of privacy self-regulation, this Article explores a different way of thinking about self-regulation based on the idea of "co-regulation." In co-regulatory approaches, industry enjoys considerable flexibility in shaping self-regulatory guidelines, while government sets default requirements and retains general oversight authority to approve and enforce these guidelines.[7] This approach to privacy self-regulation has much in common with the idea of a privacy safe harbor, which Congress first introduced in the Children's Online Privacy Protection Act of 1998 (COPPA), but re-designs it in several critical ways.

Although American scholars and regulators have previously studied the uses and limitations of self-regulation in achieving

---

[4] *See* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1524–27 (2000); CHRIS JAY HOOFNAGLE, ELEC. PRIVACY INFO. CTR., PRIVACY SELF-REGULATION: A DECADE OF DISAPPOINTMENT 11 (2005), *available at* http://epic.org/reports/decadedisappoint.pdf.

[5] *See* Swire, *supra* note 1.

[6] Darren Sinclair, *Self-Regulation Versus Command and Control? Beyond False Dichotomies*, 19 LAW & POL'Y 529, 532 (1997); *see also* Neil Gunningham & Joseph Rees, *Industry Self-Regulation: An Institutional Perspective*, 19 LAW & POL'Y 363, 363 (1997).

[7] *See* Sinclair, *supra* note 6, at 544.

information privacy,[8] they have thus far given little systematic attention to safe harbors or co-regulatory initiatives generally.[9] This Article argues that co-regulation, including privacy safe harbors, is an effective and flexible policy instrument that, if properly designed, offers several advantages as compared to the false dichotomy of voluntary industry guidelines versus prescriptive government regulation. First, the existing COPPA safe harbor, without any modification, deals successfully with virtually all of the standard criticisms of self-regulation.[10] Second, by allowing greater flexibility in structuring self-regulatory frameworks, Congress can enable the FTC to experiment with policy innovations such as Privacy-Enhancing Technologies (PETs) and new ways of implementing FIPPs to better address difficult issues such as behavioral advertising.[11] Finally, by using the right combination of sticks and carrots to re-design privacy safe harbors, Congress can encourage much broader industry participation, thereby ensuring a baseline level of monitoring and dispute resolution, while allowing the FTC to devote its scarce enforcement resources to the most egregious or systemic privacy abuses.[12]

Why does this matter? For the first time in ten years, Congress seems ready to revisit comprehensive online privacy legislation. Leading technology firms have voiced support for a privacy law and have joined with privacy groups to draft model legislation.[13] The House Committee on Energy and Commerce held several hearings on data privacy and security issues. In 2010, (former) Rep. Boucher

---

[8] *See* Swire, *supra* note 1.

[9] One exception is Peter P. Swire, *Reply: Safe Harbors and a Proposal to Improve the Community Reinvestment Act*, 79 VA. L. REV. 349, 371-78 (1993) (offering preliminary thoughts towards a general theory of safe harbors as a regulatory mechanism). For a review of European scholarship on co-regulation, *see, e.g.*, HANS-BREDOW-INSTITUT, FINAL REPORT: STUDY ON CO-REGULATION MEASURES IN THE MEDIA SECTOR (2006), *available at* http://ec.europa.eu/avpolicy/docs/library/studies/coregul/final_rep_en.pdf.

[10] *See infra*, Part III.C.

[11] *See infra*, Part IV.A and B.

[12] *See infra*, Part IV.C.

[13] *See* Joelle Tesler, *Microsoft, Google Back Privacy Legislation*, MSNBC (July 10, 2008), http://www.msnbc.msn.com/id/25622863 (last visited July 12, 2011).

circulated a draft discussion bill[14] and Rep. Rush introduced a new data privacy bill, H.R. 5777, which has since been reintroduced as H.R. 611.[15] If Congress enacts either bill, one might reasonably assume that self-regulatory initiatives would fade away. But this need not be the case. For example, the COPPA safe harbor provision sought to encourage participation in self-regulatory programs by treating a company that follows program guidelines as having complied with statutory requirements.[16] This is also not an isolated example. During the 106th and 107th Congresses, which were when the Senate and the House last gave serious consideration to comprehensive privacy legislation, several of the leading bills included provisions for a self-regulatory safe harbor.[17] While the Boucher draft discussion bill includes a safe harbor provision exempting online advertisers from certain consent requirements,[18] H.R. 611 includes a full-fledged safe harbor program.[19] This Article argues that a safe harbor provision would strengthen whatever bill emerges from current discussions and further that consumers will enjoy a higher level of privacy protection under redesigned, more innovative forms of safe harbors than if Congress relied solely on the conventional enforcement model or enacted no law at all.

---

[14] *See* STAFF OF RICHARD BOUCHER, STAFF DISCUSSION DRAFT 8–19 (2010), *available at* http://dataprivacy.foxrothschild.com/stats/pepper/orderedlist/downloads/download.php?file=http%3A//dataprivacy.foxrothschild.com/uploads/file/Privacy_Draft_5-10.pdf.

[15] *See* Best Practices Act, H.R. 5777, 111th Cong. (2010), *available at* http://www.house.gov/rush/pdf/BPACT_004.pdf; *see also* Building Effective Strategies to Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards Act (BEST PRACTICES), H.R. 611, 112th Cong. (2011), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=112_cong_bills&docid=f:h611ih.txt.pdf.

[16] This is referred to as "deemed compliance." *See infra,* note 154 and accompanying text. European and Australian privacy laws create a similar mix by requiring substantive standards for the protection of personal data while also encouraging co-regulation with industry sectors. *See infra* notes 172–176 and accompanying text.

[17] *See, e.g.*, Electronic Privacy Bill of Rights Act of 1999, H.R. 3321, 106th Cong. § 4 (1999); Online Privacy Protection Act of 1999, S. 809, 106th Cong. § 3 (1999); Consumer Privacy Protection Act of 2002, H.R. 4678, 107th Cong. § 106 (2002); Online Personal Privacy Act, S. 2201, 107th Cong. § 203 (2002).

[18] *See* STAFF OF RICHARD BOUCHER, *supra* note 14, § 3(e).

[19] *See* H.R. 611, *supra* note 15, §§ 401–04, which sets forth a Safe Harbor Self-Regulatory Choice Program.

The Article has four parts. Part I analyzes the privacy debate over the past 15 years and shows that the differences between proponents of voluntary codes and those favoring prescriptive regulation are irreconcilable, largely due to reliance on the false dichotomy of regulatory options. Next, Part II analyzes the various types of self-regulation and describes a more collaborative, flexible, and performance-based approach, drawing on critical insights from environmental regulation. This Part concludes by articulating a normative framework for assessing self-regulatory programs consisting in six factors: efficiency, openness and transparency, completeness, strategies to address free rider problems, oversight and enforcement, and use of second-generation design features. Part III then applies this normative framework to four case studies: the first is a voluntary industry code aimed at online behavioral advertising practices; the second is a government-sponsored safe harbor program resulting from inter-governmental efforts to ensure data flows between Europe and the U.S.; the third is a statutory safe harbor under COPPA, which is designed to facilitate industry self-regulation as a vital component of protecting children's privacy; and the fourth explores privacy covenants. The assessment of these case studies against the six factors leads to the conclusion that while statutory safe harbors and privacy covenants are the most promising forms of self-regulation, they still suffer from some critical weaknesses. Finally, Part IV relies on the preceding analysis to propose more sophisticated versions of privacy covenants and a revamped version of statutory safe harbors. The Article concludes by recommending that Congress adopt these new tools to help protect online consumer privacy.

I. THE PRIVACY DEBATE

When the Clinton Administration began to develop a regulatory framework for electronic commerce and the Internet, it promoted self-regulation as the preferred approach to protecting consumer privacy online. Clinton officials believed that private sector leadership would cause electronic commerce to flourish, and specifically supported efforts "to implement meaningful, consumer-friendly, self-regulatory privacy regimes" in combination with technology solutions.[20] While arguing that unnecessary regulation might distort market developments by "decreasing the supply and raising the cost of

[20] *See* WILLIAM J. CLINTON & ALBERT GORE, JR., A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE 18 (1997).

products and services" or by failing to keep pace with "the break-neck speed of change in technology,"[21] they also asserted that if industry failed to address privacy concerns through self-regulation and technology, the pressure for a regulatory solution would increase.

Not surprisingly, industry embraced this view. For example, at a 1995 public privacy workshop, industry representatives cited three reasons that regulating privacy would be counterproductive. First, it would stifle innovation in a developing market. Second, it might drive marketing activity off the Internet entirely by adding unnecessary costs to online advertising. And third, it would interfere with the market definition of consumer privacy preferences and the appropriate industry response.[22] Privacy advocates in attendance expressed a contrary view, warning that self-regulation would remain ineffective without enforceable privacy rights, which were necessary to deter bad actors and outliers and ensure the widest possible participation in any self-regulatory schemes, also noting that technology alone was no substitute for enshrining FIPPs in law.[23]

Over the next fifteen years, the two sides in the debate have largely held fast to their views, Congress has tried and failed to enact online privacy legislation, and the FTC has fluctuated between supporting legislation and giving self-regulation yet another try. What is most striking about the ensuing privacy debate is neither the opposing views of advocates and industry nor the FTC's ambivalence. Rather, it is the assumption at the heart of the debate that policy makers must choose exclusively between these two options. This is a false dichotomy and one that neglects the wide variety of co-regulatory alternatives that could be playing a larger role in the privacy arena.

In the mid-1990s, industry and its supporters placed less value on privacy than on market goals such as efficiency, flexibility, and competitiveness. A number of economists and privacy scholars with a free-market perspective developed the intellectual underpinnings of this way of thinking by emphasizing three main points: (1) the social and economic benefits that flow from "readily accessible information about consumers" and the corresponding harm that would result from privacy law to the extent that it interfered with such open information

---

[21] *Id.* at 4.

[22] *See* FED. TRADE COMM'N, STAFF REPORT: PUBLIC WORKSHOP ON CONSUMER PRIVACY ON THE GLOBAL INFORMATION INFRASTRUCTURE 27–29 (1996), *available at* http://www.ftc.gov/reports/privacy/privacy.pdf.

[23] *Id.*

flows;[24] (2) the extent to which a consent requirement regarding the collection, use or transfer of personal information "burdens consumers and creates costs";[25] and (3) the belief that industry had compelling market incentives for addressing customer privacy concerns through self-regulatory measures.

Neoclassical economists such as Paul Rubin and Thomas Lenard took this last point a step further by arguing that "market forces are moving rapidly to provide the privacy desired by consumers, in part by eliminating problems of asymmetric information."[26] For support, they pointed to numerous examples of adverse publicity forcing firms accused of violating consumers' privacy expectations to modify their data collection practices or to cancel their plans to combine or use data in new ways.[27] Rubin and Lenard also claimed that the Internet is premised on the exchange of free content and services in return for personal information used mainly for advertising and marketing purposes and that there was little evidence that legal uses of information for such purposes harm consumers. Accordingly, they concluded that "the potential benefits of new privacy regulations are very small."[28]

---

[24] *See Privacy in the Commercial World: Hearing Before the Subcomm. on Commerce, Trade and Consumer Protection Comm. on Energy and Commerce*, 107th Cong. 17–26 (2001) (statement of Professor Fred H. Cate) (citing benefits such as the ready availability and low cost of consumer credit, more convenient customer services, more relevant advertising and marketing materials, and better fraud detection and prevention).

[25] *See Need for Internet Privacy Legislation: Hearing Before the S. Comm. on Commerce, Science and Transportation*, 107th Cong. 18–28 (2001) (statement of Professor Fred H. Cate) (arguing that consent requirements are costly because consumers tend to ignore privacy notices, whatever their form, but that opt-out rules were preferable because they at least preserved the flow of information). For a more detailed treatment, *see* FRED H. CATE, PRIVACY IN PERSPECTIVE (2001). *See also* Swire, *supra* note 1 (describing additional costs associated with privacy regulation such as (1) administrative costs on government and taxpayers to draft, oversee, and enforce privacy rules; and (2) compliance costs on industry due to the inevitable lack of precision and inflexibility of government rules).

[26] PAUL H. RUBIN & THOMAS M. LENARD, PRIVACY AND THE COMMERCIAL USE OF PERSONAL INFORMATION 49 (2001).

[27] *Id.* at 51. More recently, Google responded to privacy concerns raised by its new Buzz social network service by changing its feature within a week of launch. *See* David Coursey, *Google Apologizes for Buzz Privacy Issues*, PC World (Feb. 15, 2010), http://www.pcworld.com/businesscenter/article/189329/google_apologizes_for_buzz_privacy_issues.html (last visited July 12, 2011).

[28] RUBIN & LENARD, *supra* note 26, at 64. For contemporaneous studies by other economists reaching similar conclusions, *see* Robert E. Litan, *Balancing Costs and Benefits of New Privacy Mandates* 14–17 (AEI-Brookings, Working Paper No. 99–03,

On the other side of the debate, privacy scholars Jerry Kang and Paul Schwartz sought to rebut these arguments by demonstrating the existence of a privacy market failure, which they analyzed in terms of two related ideas: information asymmetries and collective action problems. In Kang's view, information asymmetries exist because "individuals today are largely clueless about how personal information is processed through cyberspace."[29] Moreover, consumers face a collective action problem because they find it difficult to band together to bargain for better privacy practices due to their large numbers, lack of repeat play, and difficulty in locating like-minded individuals.[30] According to Schwartz, a third reason for skepticism about market-based privacy standards is the "consent fallacy"—that is, the lack of either informed or voluntary consumer consent to the privacy practices of websites.[31] Schwartz argues that the resulting market failure awards a subsidy to companies that exploit personal data, leading them to over-invest in collecting and tracking such data and to under-invest in privacy protection. The only way to end this subsidy is to establish a new default norm of minimal data disclosure—something industry has no reason to pursue because it prefers "weak standards that ratify the current status quo or even weaken it."[32] In

---

1999), *available at* http://papers.ssrn.com/abstract_id=179074; Robert W. Hahn & Anne Layne Farrar, *The Benefits and Costs of Online Privacy Legislation*, 54 ADMIN. L. REV. 85, 119–20 (2002). For an industry perspective, *see* Kent Walker, *The Costs of Privacy*, 25 HARV. J.L. & PUB. POL'Y 87, 87-88 *(2001)*; J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109 (2008) (emphasizing the value of information exchange and the need to base privacy regulation not on FIPPs but on "the potential consequences for consumers of information use and misuse").

[29] Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1253 (1998).

[30] *Id.* at 1254–56; *see* Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*, *supra* note 1.

[31] Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 833 (2000).

[32] *Id.* at 847; *see also* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1686 (1999). In questioning the market's capacity to protect privacy, Kang and Schwartz (like a great many other privacy scholars) also call attention to the invasive nature of the Internet. Kang points out that "[t]he very technology that makes cyberspace possible also makes detailed, cumulative, invisible observation of our selves possible." This constant surveillance "leads to self-censorship" and undermines human dignity. Kang, *supra* note 29, at 1198 & 1260. For Schwartz, the creation, combination, and sale of finely granulated personal data that most people are unable to control results in what he calls the "privacy horror show." Unlike Kang, his chief focus is the impact of excessive information processing on democratic deliberation and an individual's capacity for self-rule. *See*

short, Schwartz agrees with Kang that federal legislation is needed to correct the market failure and overcome weak self-regulatory standards.[33]

As scholars staked out opposing sides in the early years of this debate, the FTC's position evolved from guarded enthusiasm for self-regulation (which it described in 1999 as "the least intrusive and most efficient means to ensure fair information practices, given the rapidly evolving nature of the Internet and computer technology");[34] to growing doubt over whether self-regulatory initiatives were succeeding;[35] to formally recommending that Congress enact comprehensive online privacy legislation.[36] But, as of this writing, Congress has yet to enact such legislation.

Schwartz, 52 VAND. L. REV. 1609, at 1621–32 & 1647–67. For an updated discussion of this point, *see* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 27–55 (2004).

[33] *See* Schwartz, *supra* note 31, at 854–57 (applauding COPPA and supporting opt-in requirements in privacy laws); Kang, *supra* note 29, at 1271–73 (arguing that both advertising and other secondary uses of personal information should be permitted only with statutorily-imposed opt-in consent).

[34] FED. TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE: REPORT TO CONGRESS 6 (1999), *available at* http://www.ftc.gov/os/1999/07/privacy99.pdf (characterizing a view stated in an earlier report); *see also* FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS (1998), *available at* http://www.ftc.gov/reports/privacy3/toc.shtm [hereinafter FTC, PRIVACY ONLINE REPORT].

[35] These doubts arose after the FTC surveyed commercial websites' privacy practices and found that only 14% of websites collecting personal information from consumers had privacy notices and only 2% had a "comprehensive" privacy policy. Based on its analysis of this data, the Commission concluded "the vast majority of online businesses have yet to adopt even the most fundamental fair information practice (notice/awareness)." *See* FTC, PRIVACY ONLINE REPORT, *supra* note 34, at 4. In Congressional testimony a few months later, then-FTC Chairman Robert Pitofsky characterized industry's self-regulatory initiatives as "inadequate and disappointing" and recommended that Congress enact online privacy legislation unless industry demonstrated significant progress by the end of 1998. *See Electronic Commerce: Privacy in Cyberspace: Hearing on H.R. 2368 Before the Subcomm. on Telecomms., Trade and Consumer Protection of the House Comm. on Commerce*, 105th Cong. (1998) (statement of Robert Pitofsky, Chairman, Fed. Trade Comm'n), *available at* http://www.ftc.gov/os/1998/07/privac98.htm.

[36] In 2000, the FTC, by a 3–2 majority, recommended that Congress enact an omnibus privacy law. *See* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: REPORT TO CONGRESS 36 (2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf. In part, this recommendation hinged on the results of a second survey of website privacy practices that once again demonstrated industry's failure to achieve broad adoption of self-regulatory initiatives. Commissioner Orson Swindle dissented, stating that among the many deficiencies in the

The next phase in the FTC's position occurred in 2001, when President Bush appointed Tim Muris as FTC Chair and he shelved the regulatory debate in favor of a new privacy agenda. This new agenda was designed to protect consumers against the risk of economic injuries (such as identity theft, phishing, and data breaches) and threats of unwanted intrusions (such as online stalking, telemarketing, and spam).[37] Over the next eight years, Muris and his successors at the FTC focused on reducing the harms associated with information misuse and abuse, mainly through new programs (such as the hugely popular "Do-Not-Call List"), more enforcement actions, and consumer outreach. While the Commission continued to believe in self-regulation as part of its broader agenda, it confined its work in the privacy arena to problems causing specific harms and to laws that enhanced its enforcement powers.[38]

A third phase emerged in 2006 when the FTC began to explore the likely impact of technology and market changes on consumers and, for the first time in many years, identified "self-regulatory initiatives" as one of its primary objectives.[39] Over the next two years, the Commission renewed its earlier focus on the privacy issues associated with online behavioral advertising (OBA) and embraced self-regulatory guidelines for OBA as the best way forward.[40]

2000 report, "there is absolutely no consideration of the costs and benefits of regulation." *Id.* at 16 (dissenting Statement of Orson Swindle, FTC Commissioner).

[37] *See* Timothy J. Muris, Chairman, Fed. Trade Comm'n, Remarks at the Privacy 2001 Conference (Oct. 4, 2001), *available at* http://www.ftc.gov/speeches/muris/privisp1002.shtm. In his remarks, Muris was quite skeptical about the wisdom of enacting new online privacy legislation, questioning "how such legislation would work and the costs and benefits it would generate."

[38] *See, e.g.*, CAN-SPAM Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (codified at 15 U.S.C. §§ 7701–7713 and 18 U.S.C. § 1037) (authorizing the FTC to enforce violations of the Act); *see also* U.S. SAFE WEB Act of 2006, Pub. L. No. 109 –455, 120 Stat. 3372 (codified in scattered sections of 15 U.S.C. and at 12 U.S.C. § 3412) (enhancing the FTC's ability to conduct investigations into illegal spam, spyware, and cross-border fraud and deception, and to cooperate with its foreign counterparts).

[39] FED. TRADE COMM'N, PROTECTING CONSUMERS IN THE NEXT TECH-ADE 4, 9, & 11 (2008), *available at* http://www.ftc.gov/os/2008/03/P064101tech.pdf (the other area was protecting minors who use social networking websites). Although the agency published this report in the spring of 2008, it referred to a set of public hearings held in November 2006. At these hearings, witnesses also mentioned self-regulatory efforts in the mobile device industry and by developers of RFID devices.

[40] *See, e.g.*, FED. TRADE COMM'N, ONLINE BEHAVIORAL ADVERTISING: MOVING THE DISCUSSION FORWARD TO POSSIBLE SELF-REGULATORY PRINCIPLES 3–6 (2007) *available at* http://www.ftc.gov/os/2007/12/P859900stmt.pdf; *see also* FED. TRADE COMM'N, STAFF

And yet in 2009, no sooner did Jon Leibowitz become President Obama's new FTC Chair, then he began to express doubts about the efficacy of the self-regulatory approach. Noting that the current behavioral advertising guidelines did not seem to be working, he alluded to the recently issued Staff Guidelines on self-regulatory principles for OBA and expressed hope that industry would respond with concrete improvements. "Self-regulation, if it works, can be the fastest and best way to change the status quo," he stated, at the same time warning his audience, "If there isn't an appropriately vigorous response, my sense is that Congress and the Commission may move toward a more regulatory model."[41]

As Yogi Berra famously said, "This is déjà vu all over again." As shown above, several earlier FTC Chairs arrived at exactly this point only to reluctantly conclude that self-regulation would not work. One may offer various explanations for Leibowitz's change in heart, ranging from politics,[42] to dissatisfaction with both the traditional notice and choice model *and* the harms-based approach,[43] to a lingering concern over the unintended consequences that might result from ill-conceived regulation of online advertising.[44] An alternative

---

REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING: TRACKING, TARGETING, AND TECHNOLOGY (2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf [hereinafter Staff Report on Self-Regulatory Principles]. In familiar words, this report characterized self-regulation as providing "the necessary flexibility to address evolving online business models." *Id.* at 11.

[41] JON LEIBOWITZ, CHAIRMAN, FED. TRADE COMM'N, REMARKS AT THE CENTER FOR DEMOCRACY AND TECHNOLOGY GALA (Mar. 10, 2009), *available at* http://www.ftc.gov/speeches/leibowitz/090310remarksforcdtdinner.pdf (last visited Mar. 9, 2011).

[42] *See* Robert R. Belair, Presentation at the Harvard Symposium on Privacy and the 110th and 111th Congresses, Congressional Privacy Policy Panel (Aug. 21, 2008), *available at* http://www.ehcca.com/presentations/HIPAA16/belair_3.ppt (last visited Mar. 9, 2011) (noting that privacy legislation has never enjoyed reliable political support, especially given the relatively strong opposition from parts of industry and the jurisdictional complications that inevitably arise when multiple committees lay claim to privacy initiatives).

[43] *See* Stephanie Clifford, *Fresh Views at Agency Overseeing Online Ads*, N.Y. TIMES, Aug. 5, 2009 at B5; *see also An Interview With David Vladeck of the F.T.C.* (Aug. 5, 2009), http://mediadecoder.blogs.nytimes.com/2009/08/05/an-interview-with-david-vladeck-of-the-ftc/ (last visited July 12, 2011) [hereinafter Vladeck Interview] (citing statements by David Vladeck, the new Director of the Bureau of Consumer Protection, in which he questions both the notice and consent framework and the harms-based framework).

[44] *See* Robert E. Litan, *Law and Policy in the Internet Age*, 50 DUKE L.J. 1045, 1065 (2001) (pointing out that statutory requirements may increase "the costs of marketing, leading to

view pursued in this Article is that the best way to avoid the recurring pattern of encouraging self-regulation and then doubting its effectiveness as described above is to overcome the false dichotomy in the privacy debate between self-regulation in the form of largely voluntary industry codes and restrictive federal privacy legislation as the sole alternatives. It should be clear from the above discussion that there is an important role for regulation to play in the protection of personal data, especially given the frequently disappointing results of industry self-regulatory efforts. At the same time, it is equally clear that the costs of prescriptive regulation are at present unknown, could be very significant, and could have a deleterious effect on the success of existing business models and/or the future growth of the information technology sector. This suggests the importance of finding new regulatory mechanisms that both do a good job of protecting personal data, and do so in a cost-effective and flexible way. The next section explores which forms of self-regulation (if any) could, potentially, play this role.[45]

II. REGULATORY INNOVATION

Modern regulatory theory is founded on two basic propositions. The first is that traditional forms of state regulation based on detection and prosecution of violations of government-issued rules is inadequate for a host of reasons: it is costly, inefficient, intrusive, disregards the unique interests of individual firms in favor of a "one-size-fits-all" approach, fails to harness industry expertise, and stifles innovation.[46] The second is that self-regulation has distinct advantages over state regulation, including greater flexibility, lower program costs, and higher compliance levels, which also enables

---

increased costs for products and possibly reduced choice . . . for consumers" if some sites are forced to cut back on the availability of free online content and services).

[45]The need for new regulatory models is a recurring theme in the recent work of both U.S. and European privacy officials. *See* Edward Wyatt & Tanzina Vega, *Stage Set for Showdown on Online Privacy*, N. Y. TIMES, Nov. 10, 2010, at B1 & B6 (noting that both the FTC and the DOC will be issuing reports on online privacy before the end of 2010 and that the EC recently issued a preliminary report describing needed changes in E.U. privacy laws).

[46] See Gunningham & Rees, supra note 6, at 364; Sinclair, *supra* note 6, at 530; IAN AYRES & JOHN BRAITHWAITE, RESPONSIVE REGULATION: TRANSCENDING THE DEREGULATION DEBATE 35–51 & 106 (Donald R. Harris et al. eds., 1992).

regulators to focus more on "bad" actors.[47] At the same time, it is well understood that self-regulation is unlikely to live up to its promise unless there is some mechanism for constraining economic self-interest. This implies a need for selective government involvement in rulemaking (e.g., setting default requirements) and enforcement (e.g., requiring disclosure of performance and periodic assessment by the state).[48] And the weight of scholarly opinion suggests that such "co-regulatory" solutions, which combine a self-regulatory mechanism with some form of state intervention, "are more resilient and effective than self-regulation in isolation."[49] This Part begins by examining the forms of self-regulation and their primary characteristics. Next, it introduces the idea of regulatory covenants and gives an overview of two kinds of environmental covenants that offer lessons for privacy regulation—Project XL and regulatory negotiations. Finally, it develops a normative framework for evaluating self-regulatory privacy schemes. These normative insights also point the way towards a more successful co-regulatory approach to protecting personal data.

A. TYPES OF SELF-REGULATION

Self-regulation defies easy definition, but at a minimum involves a professional or private organization assuming responsibility for its own rules and sanctions rather than being publicly regulated by government. As noted earlier, it is a malleable term and may take many different forms.[50] One of the most common ways of distinguishing different forms of self-regulation is to place them on a continuum based on what role the government plays in regulatory rulemaking and enforcement. Joseph Rees, for example, identifies

---

[47] *See* Gunningham & Rees, *supra* note 6, at 366; AYRES & BRAITHWAITE, *supra* note 46, at 103–106. *See also* Margot Priest, *The Privatization of Regulation: Five Models of Self-Regulation*, 29 OTTAWA L. REV. 233, 268–71(1997–98) (noting that self-regulation is also politically attractive because it allows a government "to reassure critics that an area is being regulated . . . while not having to take direct responsibility for the regulatory regime").

[48] *See* AYRES & BRAITHWAITE, *supra* note *46*, at 106 (arguing that firms participating in a voluntary program will alter their behavior if doing so is cost-neutral or has only short-term costs, but not if they must incur long-term costs); *see also* Priest, *supra* note 47, at 271–74; Gunningham & Rees, *supra* note 6, at 366 & 370.

[49] Gunningham & Rees, *supra* note 6, at 366.

[50] *See* Sinclair, *supra* note 6, at 532; *see also* Gunningham & Rees, *supra* note 6, at 364.

three main forms of self-regulation.[51] One is voluntary self-regulation, in which private firms carry out both tasks independent of direct government involvement.[52] The second and third are versions of what Rees calls mandated self-regulation,[53] which privatizes both rulemaking *and* enforcement ("full" self-regulation) or limits privatization to either one of the regulatory functions but not both ("partial" self-regulation). The mandatory aspect of these two forms comes about through a legal requirement that firms self-regulate.[54] Mandatory self-regulation therefore explicitly recognizes the importance of the firm's internal compliance system in areas such as occupational safety, where it is recognized that government lacks the resources to inspect, monitor, and closely enforce safety in millions of workplaces. Rather, it may be more effective for government to rely on a firm's own safety system while creating incentives to ensure that firms comply with relevant government standards.[55]

Margot Priest adopts a similar typology that distinguishes different forms of self-regulation in terms of the degree of government involvement, as well as several additional characteristics.[56] She refers to the form of self-regulation with the least government involvement as voluntary codes of conduct, which are established by a group of like-minded firms or by a trade association as a condition of

---

[51] JOSEPH V. REES, REFORMING THE WORKPLACE: A STUDY OF SELF-REGULATION IN OCCUPATIONAL SAFETY 9–12 (1988).

[52] The most prevalent form of privacy self-regulation in the U.S. is voluntary self-regulation. Familiar examples include the Privacy Promise of the Direct Marketing Association (DMA), the Individual Reference Service Group (IRSG) Principles (which apply to data brokers), the Network Advertising Initiative (NAI) Principles (which apply to online ad firms), the privacy seal programs of Truste and BBBOnline, the Online Privacy Alliance (OPA) Guidelines, and various in-house programs of large multinationals such as Microsoft and Google.

[53] REES, *supra* note 51, at 10.

[54] *Id.* at 11.

[55] Rees's book explores a regulatory experiment carried out in the early 1980s by the Occupational Safety and Health Administration (OSHA) called the Cooperative Compliance Program (CCP). This involved a three-way arrangement among unions, management, and OSHA, in which the agency authorized labor-management safety committees to assume many of OSHA's regulatory responsibilities at several large construction sites while the agency ceased routine compliance inspections and pursued a more cooperative relationship with the participating firms.

[56] *See* Priest, *supra* note 47, at 240–41 (identifying ten characteristics).

membership. The participating firms agree to operate according to rules and procedures as defined by the code, which typically reflects industry best practices. Like voluntary self-regulation as defined by Rees, firms (or their trade associations) handle virtually all of the regulatory functions ordinarily reserved for government. Thus, participating firms are *accountable* to each other or the trade association but not to government; they engage in *rulemaking* consensually by members who adopt the code; there is neither *adjudication* (except perhaps by a peer review committee) nor a dispute resolution mechanism, and only limited *sanctions* apart from dismissal by the trade association; and *coverage* of relevant industry principles suffers from free rider problems due to the voluntary nature of the regulatory regime. Finally, there is little *public involvement*, although firms developing a code may engage in public consultation at their discretion.[57]

At the opposite end of the scale, Priest refers to the form of self-regulation with the highest degree of government involvement as "regulatory self-management." She cites several examples of regulatory self-management based on Canadian and U.S. health, safety, and environmental programs in which the legislature "gives the responsibility for the delivery of regulatory programs" to industry.[58] Although government remains responsible for rulemaking and enforcement, it directs industry to implement a regulatory program through "the application of rules and monitoring of compliance" by a nonprofit self-management organization (SMO), which industry forms to fulfill these responsibilities. Thus, in a regulatory self-management scheme, the SMO remains accountable to government for its performance and conduct; government engages in rulemaking, but may consult with the SMO as to applicable industry or firm guidelines; the SMO handles adjudication through a dispute resolution process and imposes sanctions; and the approach avoids free rider problems because all regulated entities must be part of an SMO. Finally, because the government issues applicable rules, public involvement occurs as part of the rulemaking process (i.e., via notice and comment) although a SMO might also have a public representative as a member of its Board.[59]

---

[57] *Id.* at 242.

[58] One of the three variants of regulatory self-management Priest identifies is mandatory self-regulation. *See* REES, *supra* note 51.

[59] Priest, *supra* note 47, at 251–62.

What matters for present purposes is less the details of regulatory self-management or the other intermediate forms of self-regulation identified by Priest, and more their common characteristics and how they contrast with voluntary codes. All of the former are co-regulatory solutions in the sense that they involve a combination of direct government regulation and private sector activity. Rees captures this well when he describes mandatory self-regulation as "a *governmental* strategy for strengthening *private* regulatory systems."[60]

More generally, all forms of co-regulation have several common characteristics. First, they tend to be cooperative rather than adversarial, taking full advantage of corporate social responsibility as a motivating factor in firm behavior.[61] Second, co-regulatory models rely on firms or intermediaries (such as trade associations, independent auditors, and other third parties) to perform a variety of government functions.[62] Third, co-regulatory guidelines are less prescriptive than state regulations (which tend to define required actions) and more open-ended (stating broad intentions or a desired outcome), thereby allowing regulated firms more discretion in developing specific implementation plans.[63] Fourth, firms tend to be more committed to rules that they had a hand in shaping, resulting in increased compliance rates.[64] Finally, co-regulation shifts the role of government from one of rulemaking and imposing sanctions when industry violates these rules, to that of providing incentives for implementing self-regulatory programs while maintaining "a credible residual program" of oversight and enforcement.[65] What distinguishes these co-regulatory strategies from voluntary codes is not only the degree of government involvement but, as noted above, differences in accountability, rulemaking, adjudication, sanctions, and public involvement.

---

[60] REES, *supra* note 51, at 10 (further noting that the purpose of mandatory self-regulation "is to build into the social structure of the regulated enterprise a sustained and effective commitment to insecure or precarious values—such as environmental protection, affirmative action, [or] occupational safety").

[61] *See* Douglas C. Michael, *Cooperative Implementation of Federal Regulations*, 13 YALE J. ON REG. 535, 541–42 (1996).

[62] *See* Priest, *supra* note 47, at 238.

[63] *See* Michael, *supra* note 61, at 544.

[64] *See* AYRES & BRAITHWAITE, *supra* note 46, at 113.

[65] Michael, *supra* note 61, at 541.

B. REGULATORY COVENANTS

In a path-breaking article published in 2006, Dennis Hirsch discusses the possibilities of developing a new model for privacy regulation based on a number of innovative environmental policy tools that have emerged over the past thirty years. Hirsch begins by contrasting the older, command-and-control model of environmental regulation (in which regulators both *command* the level of required performance and *control* the means of achieving it) with "second generation" regulations that encourage "the regulated parties themselves to choose the means by which they will achieve environmental performance goals" resulting in "more cost-effective and adaptable" strategies.[66] The defining characteristic of second-generation strategies is that they "allow these self-directed actions to count towards regulatory compliance." This radical departure from a command-and-control regime spurs regulatory innovation by harnessing a firm's own ingenuity in devising environmental solutions that meet or exceed legal requirements yet fit a firm's business model and the needs of its customers.[67]

Hirsch contends that privacy regulation has much to learn from these second-generation environmental strategies and he proposes several ideas for adapting them to protect information privacy without deterring innovation. His most relevant idea for present purposes is a form of co-regulation known as environmental covenants. In general, environmental covenants are contractual agreements between regulators and regulated firms. These negotiations may take place in either of two contexts: (1) where government already regulates the relevant area, or (2) where government is threatening to regulate an area but has not yet done so. Other stakeholders, such as environmental advocacy groups or members of the public, frequently have a seat at the bargaining table. In both cases, the goal is to achieve

---

[66] *See* Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 GA. L. REV. 1, 8 (2006). For a comprehensive analysis of second-generation environmental strategies, *see generally* Richard B. Stewart, *A New Generation of Environmental Regulation?*, 29 CAP. U. L. REV. 21, 38–151 (2001); *see also* DANIEL J. FIORINO, THE NEW ENVIRONMENTAL REGULATION 19–21 (2006).

[67] On the other hand, enforcement becomes more challenging when firms choose how and when to achieve regulatory goals as opposed to following a uniform national standard. Thus, these innovative strategies work best when there are reliable monitoring technologies available to measure actual pollution releases and less well when such technologies are not as well developed. *See* Hirsch, *supra* note 66, at 37–40; *see also* FIORINO, *supra* note 66, at 139.

greater flexibility and responsiveness to specific conditions and more rapid improvements than would otherwise occur under prescriptive government regulation (threatened or existing). Industry finds these covenants attractive because they have more input into the final agreement than with conventional rulemaking efforts; the covenants take the form of performance goals rather than technology mandates; and their longer time frame better fits the normal business planning and investment cycle, while government and society benefit from this approach by achieving better results (such as steeper pollution reductions) than might otherwise be politically achievable.[68] In the U.S., environmental covenants take two distinct forms depending on whether agreements are specific to an individual firm (Project XL) or result from negotiation with an industry sector (negotiated rulemaking).

Before considering these two distinct forms of covenants below, it is worth pausing to ask why the covenanting approach potentially achieves better solutions to environmental problems than command-and-control regulations. Stewart offers an explanation based on the logic of Coasian bargaining principles:

> The premise is that legal rules will advance society's welfare if they are voluntarily agreed to by all relevant interests. If those with a stake in the regulatory requirements—the regulated, the regulator, and perhaps third party environmental or citizen interests—agree on an alternative to the standard requirements, the agreement may be presumed to be superior to the standard.[69]

---

[68] *See* Stewart, *supra* note 66, at 60–94 (discussing examples of environmental agreements at both the industry and firm level).

[69] Stewart, *supra* note 66, at 61. On Coasian bargaining, see R.H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 6–8 (1960) (arguing that in the absence of transaction costs, mutually beneficial agreements lead to an efficient outcome regardless of any initial assignment of entitlements). As Stewart further explains:

> [E]ach party to an environmental agreement will seek to maximize its share of the gains produced by the negotiated departure from standard requirements. A regulated firm or industry will seek to use the flexibility afforded by environmental agreements to reduce compliance costs and other burdens by using alternative or innovative means that would be precluded by the default requirements, gaining flexibility as to

Similarly, other scholars explain the success of the covenanting approach in terms of the very nature of the underlying process, which emphasizes "stakeholder representation, face-to-face negotiation, [and] consensus-based decision making."[70] What both explanations have in common is a focus on information sharing, direct negotiations, self-interested mutual compromises, and voluntary agreement.

1. PROJECT XL

Project XL is a program authorizing the EPA to negotiate site-specific covenants with individual firms under which the agency would modify or relax existing regulatory requirements in exchange for enforceable commitments to achieve improved environmental results.[71] Interested firms submit initial project proposals to the EPA that satisfy very general criteria such as superior performance, cost savings, stakeholder support, innovation, transferability (to other facilities and possibly for future use in rules of national scope), and feasibility. Once the EPA approves a proposal, the applicant works with federal and state regulators on a Final Project Agreement (FPA) defining the specific steps the company will take to improve performance, the regulatory relief that will be granted, how performance will be measured, and the expected environmental

---

> the timing of compliance investments, and reducing regulatory uncertainty . . . . For their part, the regulators and environmental and citizen group third parties will seek a higher level of environmental or other benefits than would have been obtained, as a practical matter, under the standard default requirements. Regulators may also seek to reserve the authority unilaterally to impose new requirements if new environmental problems arise or the agreement for other reasons later proves environmentally inadequate . . . . It will also be necessary to structure the negotiation and representation process so as to minimize the transaction and bargaining costs that could prevent successful negotiation.

Id. at 61–62.

[70] *See* Jody Freeman & Laura I. Langbein, *Regulatory Negotiation and the Legitimacy Benefit*, 9 N.Y.U. ENVTL. L.J. 60, 71 & 132–35 (2000).

[71] *See generally,* Regulatory Reinvention (XL) Pilot Projects: Solicitation of proposals and request for comment, 60 Fed. Reg. 27,282 (May 23, 1995) [hereinafter Notice of Solicitation].

results. The EPA allows stakeholders an opportunity to comment on a draft FPA before finalizing the agreement.[72] For participating businesses, Project XL offers major benefits, including regulatory flexibility, reduced compliance costs, and greater regulatory certainty during the life of the agreement.[73] Although the EPA hoped to begin fifty pilot projects within two years of announcing Project XL,[74] it did not achieve this ambitious goal until a few years later.[75]

Despite having met agency goals, Project XL enjoys a mixed reputation. Critics point to three serious flaws in its design and implementation. First, they question the EPA's decision to refrain from establishing a "baseline" for determining superior performance, which has in turn led to overreaching by firms in requesting regulatory exemptions unrelated to the purported "improvements" as described in their XL project proposals.[76] Second, the EPA offered very little guidance as to what meaningful stakeholder participation required. Was it a variety of interested parties reaching a broad consensus that a proposed FPA protected the public interest or merely industry and government officials consulting with the local community? Moreover, national environmental groups complained that while they lacked the financial resources to participate in FPA negotiations, local community groups (whose participation the EPA favored) lacked the necessary expertise to understand the highly

---

[72] *See id.*

[73] *See* Rena I. Steinzor, *Regulatory Reinvention and Project XL: Does the Emperor Have Any Clothes?*, 26 ENVTL. L. REP. 10,527, 10,529–30 (1996).

[74] *See* Notice of Solicitation, *supra* note 71, at 27,287.

[75] *See* ENVTL. PROT. AGENCY, PROJECT XL: DIRECTORY OF PROJECT EXPERIMENTS AND RESULTS 2, *available at* http://www.epa.gov/projectxl/compoovol2/vol2_web.pdf. As of November 2000, forty-eight firms had signed FPAs and the EPA had identified seventy "innovations" within these projects. For a current listing of projects, see Envtl. Protection Agency, XL Projects, http://www.epa.gov/projectxl/projects.htm (last visited Mar. 9, 2011).

[76] *See* Steinzor, *supra* note 73 at 10,529–30; *see also* Dennis D. Hirsch, *Project XL and the Special Case: The EPA's Untold Success Story*, 26 COLUM. J. ENVTL. L. 219, 249–51 (2001) [hereinafter *Success Story*]; FIORINO, *supra* note 66, at 141. The EPA sought to address this problem by modifying its original guidance on Project XL. *See* Regulatory Reinvention (XL) Pilot Projects: Notice of Modifications to Project XL, 62 Fed. Reg. 19,872, 19,876 (Apr. 23, 1997) [hereinafter Notice of Modifications] (requiring that sponsors articulate the link between the flexibility sought and the superior environmental performance. The EPA also established a two-tier process for assessing such performance using both quantitative and qualitative benchmarks).

technical issues discussed in many XL proposals.[77] Finally, there are severe doubts as to whether the EPA had enough legal authority to approve FPAs that embodied different legal requirements from those imposed by otherwise applicable statutes and regulations.[78]

An obvious way to remedy Project XL's shortcoming would be for Congress to enact new legislation defining the environmental improvements required in every "experimental" XL project, clarifying the process for stakeholder involvement, and granting the EPA explicit authority to approve agreements that violate applicable regulatory or statutory requirements.[79] According to Hirsch, the experimental dimension of Project XL is valuable because it allows the EPA "to test out new and potentially better regulatory approaches and environmental technologies."[80] With this goal in mind, he proposes three design changes. First, rather than just encouraging industry proposals, the EPA should take the lead in identifying the innovative approaches worth testing. Second, the EPA should pursue projects consistent with its list of proposed innovations and enter into a small number of agreements for carrying out discrete regulatory experiments at a limited number of facilities, with no intention of expanding these innovations on a national basis. Finally, these "Experimental XL" projects should be rigorously evaluated by the EPA in partnership with the same diverse group of stakeholders whose ideas contributed to EPA's initial list of innovations worth testing. Those projects that survive such rigorous scrutiny might later become the basis for rulemaking or even new legislation, thereby preserving ideas that truly demonstrate superior environmental performance.[81] We will revisit Hirsch's proposal below in the discussion of innovative forms of privacy self-regulation.[82]

---

[77] *See* Steinzor, *supra* note 73, at 10,532–33; Hirsch, *Success Story*, *supra* note 76, at 251–52; FIORINO, *supra* note 66, at 141–42. The EPA also sought to address this problem by clarifying what it meant by "stakeholder involvement" and providing up to $25,000 per project to assure that necessary technical assistance was available to support meaningful participation. *See* Notice of Modifications, *supra* note 76, at 19,877–81.

[78] *See* Steinzor, *supra* note 73, at 10,535–36; Hirsch, *Success Story*, *supra* note 76, at 244–46; FIORINO, *supra* note 66, at 142.

[79] *See* Hirsch, *supra* note 76, at 225–29.

[80] *Id.* at 255.

[81] *Id.*

[82] *See infra* Part IV.A.

2. NEGOTIATED RULEMAKING

Negotiated rulemaking (also referred to as regulatory negotiation or "reg. neg.") is a statutorily-defined process by which agencies formally negotiate rules with regulated industry and other stakeholders as an alternative to conventional notice-and-comment rulemaking.[83] The core insight underlying negotiated rulemaking is that conventional rulemaking discourages direct communication among the parties, often leading to misunderstanding and costly litigation over final rules. In contrast, negotiated rulemaking brings together agency personnel and representatives of the affected interested groups to negotiate the text of a proposed rule based on (more honestly presented) shared information and willingness to compromise. If the negotiations succeed by achieving a consensus on a proposed rule, the resulting final rule should be of better quality, easier to implement, enjoy greater legitimacy, and lead to fewer legal challenges.[84]

The Negotiated Rulemaking Act of 1990 (NRA) establishes a statutory framework for negotiated rulemaking under which agencies have the discretion to bring together representatives of the affected parties in a negotiating committee (for example, industry, environmental and consumer groups, and state and local governments) for face-to-face discussions. If the committee reaches a consensus,[85] the agency can then issue the agreement as a proposed rule subject to normal administrative review processes. Proposed rules emerging from a negotiated rulemaking process are also subject to judicial review.[86] While the NRA augments Administrative

---

[83] Under the Administrative Procedure Act (APA) of 1946 (5 U.S.C. § 551 *et seq.*), conventional rulemaking generally requires publication of the proposed rule in the Federal Register, an opportunity for interested persons to comment on the proposed rule, and publication of a final rule at least 30 days prior to its effective date. *See* 5 U.S.C. § 553.

[84] *See* Negotiated Rulemaking Act of 1990 (NRA), Pub. L. No. 101-648, § 2(3)–(5), 104 Stat. 4,969 (codified as amended at 5 U.S.C. §§ 561–570); *see also* ENVTL. PROT. AGENCY, NEGOTIATED RULEMAKING FACT SHEET, *available at* www.epa.gov/adr/factsheetregneg.pdf; Philip J. Harter, *Negotiating Regulations: A Cure for Malaise*, 71 GEO. L.J. 1 (1982) (discussing negotiation as a means of breaking deadlocks produced by the conventional rulemaking process).

[85] *See* 5 U.S.C. § 562(2) (defining "consensus" as "unanimous concurrence among the interests represented" unless the committee agrees on a different definition such as general concurrence).

[86] *See* 5 U.S.C. § 563(a)(7) & 570.

Procedure Act (APA) rulemaking, it does not replace it. Indeed, most of the language of the Act is permissive.[87] If negotiations fail to reach a consensus, the agency may proceed with its own rule.

The promise of negotiated rulemaking is that by enlisting diverse stakeholders in the rulemaking process, responding to their concerns, and reaching informed compromises, better quality rules will emerge at a lower cost and with greater legitimacy.[88] Critics counter that the process not only fails to deliver its purported benefits (and then only rarely) but that its very use undermines the foundations of administrative law by shifting the decision-making function from agencies tasked with protecting the public interest to a collection of interest groups with their own private agendas.[89] In 2000, Jody Freeman and Laura Langbein published a comprehensive analysis and summary of an empirical study of negotiated rulemaking.[90] The study compared participant attitudes toward negotiated versus conventional rulemaking. Based on their analysis, they concluded that "reg. neg. generates more learning, better quality rules, and higher satisfaction than conventional rulemaking" as well as increasing legitimacy, which they defined as "the acceptability of the regulation to those involved in its development."[91] But even if this very positive analysis is taken at face value, Lubbers shows that the EPA use of negotiated rulemaking is in fact quite limited, having fallen off in recent years by almost two-thirds.[92] Despite this decline, which Lubbers attributes to budgetary issues and the burdens of complying with federal advisory committee

---

[87] *See* Jeffrey S. Lubbers, *Achieving Policymaking Consensus: The (Unfortunate) Waning of Negotiated Rulemaking*, 49 S. Tex. L. Rev. 987, 989 (2008) (noting that "the Act does not *require* the agency to publish either a proposed or final rule merely because a negotiating committee proposed it").

[88] *See* Harter, *supra* note 84.

[89] For a discussion of the main lines of criticism, *see* Lubbers, *supra* note 87, at 1003–04.

[90] *See* Freeman & Langbein, *supra* note 70, at 132–35 (presenting analysis and a summary of empirical evidence from Neil Kerwin and Laura Langbein's two-phase study of EPA negotiated rulemakings). I want to thank Peter Schuck for referring me to this article and alerting me to the relevance of the reg. neg. debate.

[91] *Id.* at 63.

[92] *See* Lubbers, *supra* note 87, at 996. Although agencies have discretion under the NRA to determine whether to rely on negotiated rulemaking provided they consider the seven factors identified in 5 U.S.C. § 563(a), Congress has mandated its use in several statutes across a range of issues. For a list of congressionally-mandated reg. neg. procedures, *see* Lubbers, *id.* at 1007–15.

requirements, Lubbers insists upon the proven value of reg. neg. in providing creative solutions to regulatory problems.[93]

Other environmental law scholars have identified a few situations where negotiated rulemaking should provide the EPA with significant advantages. For example, Andrew Morriss and his colleagues point to situations "where the substance of the regulation requires the credible transmission of information between the regulated entities and other interest groups, and where the agency's preference for a particular substantive outcome is weak."[94] Reg. neg. also requires "a relatively high degree of shared interest among the groups participating, the existence of gains from trade to allow parties to compromise, and a willingness by interest groups to reject the role of spoiler."[95] These views are largely consistent with the findings of Daniel Selmi, who conducted a detailed study of the negotiation of a regional air quality rule. Selmi explained that the parties were willing to compromise for several reasons: (1) the industry believed that regulation was inevitable; (2) the environmental groups recognized that even though they preferred an outcome based on new and expensive technology, they lacked the political capital to achieve this result; and (3) the agency was not locked into a rigid, initial position, but remained open towards finding a solution that responded to information acquired during the negotiations. But the key factor in reaching a compromise was a very practical one—namely, that the facilitator had the necessary skills to assist the parties in identifying their priorities and to help them make tradeoffs in which they each achieved some of their goals.[96]

In sum, both Project XL and negotiated rulemaking have strengths and weaknesses. Key strengths of a well-designed covenanting approach include innovation (because covenants invite firms to tap

---

[93] *Id.* at 1006 (giving the example of a recent reg. neg. involving a regional air quality rule).

[94] Andrew P. Morriss et al., *Choosing How to Regulate*, 29 HARV. ENVTL. L. REV. 179, 183 (2005).

[95] *Id.*

[96] *See* Daniel P. Selmi, *The Promise and Limits of Negotiated Rulemaking: Evaluating the Negotiation of a Regional Air Quality Rule*, 35 ENVTL. L. 415, 435–38 (2005). Scholars disagree over a much more general issue regarding the suitability of reg. neg. in any given situation. Selmi notes that some scholars "argue that controversial rules make good candidates for negotiation, while others contend the process is best utilized for narrow questions of implementation. A third group stresses that agencies should use negotiation to tackle situations where the policy implications are limited." (citations omitted). *Id.* at 467–68.

into their own ingenuity); flexibility (in the form of tailored rules that either match the circumstances of an individual firm, as in Project XL, or the underlying conditions faced by a regulated industry based on superior expertise, as in negotiated rulemaking); greater commitment (because companies write or at least negotiate their own rules rather than having them imposed externally); more effective compliance (because internal discipline as practiced by firms that agree to rules of their own devising is likely to be more extensive and cheaper for everyone than government investigations and prosecutions); and, as a result of these benefits, lower-cost solutions. On the other hand, covenants have a number of obvious weaknesses, including higher administrative burdens associated with negotiating the rules (although this might be mitigated by lower overall costs for compliance and litigation); legal uncertainty in the case of Project XL; and a bias against small firms, which typically lack the resources necessary to negotiate facility-based standards or to participate in a negotiating committee.[97]

C. NORMATIVE FRAMEWORK FOR ASSESSING SELF-REGULATORY INITIATIVES

Having identified different types of self-regulation and their co-regulatory characteristics, and having investigated environmental covenants such as Project XL and regulatory negotiations (in keeping with Hirsch's suggestion that such covenants may provide the basis for innovative approaches to privacy regulation), this Article now presents a normative framework for evaluating the effectiveness of co-regulatory programs. Part III will apply this normative framework to four instances in which regulators have used co-regulation in the field of information privacy and assess their relative merits. The normative framework developed here melds the discussion of standard public policy criteria in Part II.A with the central features of second-generation strategies as reflected in the analysis of covenants in Part II.B. The resulting framework consists of six elements that are critical to the success of co-regulatory initiatives: *efficiency, openness and transparency, completeness, strategies to address free rider problems, oversight and enforcement,* and *use of second-generation design features.*

---

[97] For a similar list of the strengths and weaknesses of enforced self-regulation, *see* AYRES & BRAITHWAITE, *supra* note 46, at 110–16 & 120–28.

1. EFFICIENCY

Efficiency may be defined as "achieving regulatory objectives at the lowest attainable cost."[98] For all forms of self-regulation, efficiencies arise from harnessing industry expertise in the development of industry codes, which are inherently more flexible than legislation and may be tailored to the circumstances of individual firms, or adjusted to changes in market conditions or new technologies. In general, self-regulation costs less for government than regulatory rulemaking and enforcement because it shifts costs to industry. Whether it costs less for industry depends on the form of self-regulation and whether industry passes on its costs to consumers.[99]

2. OPENNESS AND TRANSPARENCY

Openness refers to whether the self-regulatory system allows the public to play any role in developing the underlying rules and enforcement mechanisms. Transparency, on the other hand, is a function of a system's ability "to produce and promulgate two kinds of information: (1) information about the normative standards the industry has set for itself; and (2) information about the performance of member companies in terms of those standards."[100] In general, self-regulatory schemes publicize the existence and content of their principles (especially if their rules are determined by statute and hence publicly available). Purely voluntary codes may involve public interest groups at the discretion of member firms. When firms decide to develop codes using a consensus-based process, however, a wider range of interests is likely to be represented. Finally, performance data is not usually shared with the public and most self-regulatory organizations treat enforcement proceedings as private, but may publicly announce the outcome of any enforcement actions involving member firms.

---

[98] *See* Priest, *supra* note 47, at 274.

[99] This analysis of efficiency ignores privacy externalities, which may arise when firms fail to consider the consequences to consumers of violating their privacy. *See* Hal R. Varian, *Economic Aspects of Personal Privacy*, *in* PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (U. S. Dep't of Commerce ed., 1997), *available at* http://www.ntia.doc.gov/reports/privacy/selfreg1.htm (last visited Mar. 9, 2011).

[100] *See* Gunningham & Rees, *supra* note 6, at 383.

3. COMPLETENESS

Completeness is the straightforward matter of whether a self-regulatory code of conduct addresses all relevant aspects of the standards governing industry practices. In privacy terms, these standards are embodied in the FIPPs, which are the benchmark against which the FTC and privacy advocates evaluate any self-regulatory privacy scheme.[101] Unless they adhere to a pre-existing industry standard, voluntary codes often omit principles or practices that their members find too burdensome. In contrast, where government establishes default requirements on a statutory basis, incompleteness is rarely an issue.

4. STRATEGIES TO ADDRESS FREE RIDER PROBLEMS

Free riding occurs in voluntary programs when members enjoy the benefits of a program without having to meet its obligations. As Fiorino notes, "It reduces confidence in the reliability and quality of participants and thus affects the program's credibility."[102] There are two main versions of the free rider problem. First, some firms may agree to join a program but merely feign compliance. And second, certain firms in the relevant sector may simply refuse to join at all. Both versions are potentially fatal to self-regulatory programs because they create a competitive disadvantage for honest participants. The first version may be counteracted by "peer group pressure, shaming, or more formal sanctions" while the second may require that "government intervenes directly to curb the activities of non-participants."[103] Obviously, free rider problems dissipate when regulated entities are required to participate in a self-regulatory program or when codes of conduct are subject to government review and approval. Self-regulatory initiatives need to incorporate such strategies in order to prove effective.

5. OVERSIGHT AND ENFORCEMENT

At an early stage of the U.S. government's support for self-regulatory privacy guidelines, the DOC commissioned a study of the

---

[101] *See supra* notes 34–36 and accompanying text.

[102] FIORINO, *supra* note 66, at 125.

[103] Gunningham & Rees, *supra* note 6, at 393-94.

criteria for effective self-regulation. In addition to substantive criteria based on FIPPs, the DOC study identified three oversight and enforcement criteria: (1) consumer recourse, or the availability of affordable mechanisms for resolving complaints and perhaps awarding some compensation to an injured party; (2) verification, or the nature and extent of audits or more cost-effective ways to verify that a companies' assertions about its privacy practices are true and to monitor compliance with a program's requirements; and (3) consequences for failure to comply with program requirements, such as cancellation of the right to use a seal, public notice of a company's non-compliance, or suspension or expulsion from the program.[104] Voluntary codes are often deficient in all three components. Once again, required government approval of these oversight and enforcement mechanisms ensures that baseline regulatory objectives are met.

6. USE OF SECOND-GENERATION DESIGN FEATURES

The central features of second-generation environmental strategies are discussed at considerable length by Stewart and Fiorino.[105] For present purposes, their insights may be boiled down (however inadequately) to the following catch phrase: self-interested mutual promises that reward good actors for superior performance. These strategies presuppose direct bargaining, information sharing, and the affected parties buying-in to cost-effective and innovative regulatory solutions. In view of these characteristics, second-generation strategies such as environmental (or privacy) covenants should achieve better outcomes than either conventional rulemaking or voluntary self-regulation.

III. FOUR CASE STUDIES

This Article now presents four case studies of self-regulatory privacy schemes. The first case study focuses on the Network Advertising Initiative (NAI) Principles, a voluntary code established by an ad hoc industry advertising group that also oversees members' compliance. The second case study looks at a safe harbor solution for

---

[104] *See* U.S. DEP'T OF COMMERCE & OFFICE OF MGMT. & BUDGET, ELEMENTS OF EFFECTIVE SELF-REGULATION FOR THE PROTECTION OF PRIVACY (1998), *available at* http://www.ntia.doc.gov/reports/privacydraft/198dftprin.htm.

[105] *See supra* note 66.

U.S. firms needing to transfer data from the E.U. to the U.S. without running afoul of E.U. data protection requirements. To benefit from the safe harbor, firms have to certify that they will comply with privacy principles negotiated between the U.S. and E.U. but administered by industry seal programs. The third case study deals with FTC-approved safe harbor programs under COPPA, focusing, in particular, on that of the Children's Advertising Review Unit (CARU). Each of these three self-regulatory schemes will be classified using Priest's typology and evaluated in terms of the six factors identified above in Part II.C. The fourth and final case study begins with a brief overview of privacy covenants, both in the U.S. and abroad, and then turns to a very recent example of a voluntary covenanting approach to privacy. This last case study is less a detailed description and analysis of a specific program, and more a transitional step towards second-generation strategies.

A. THE NETWORK ADVERTISING INITIATIVE

On November 8, 1999, the DOC and the FTC held a public workshop on online profiling, which the FTC defined as the collection of data about consumers using cookies and web bugs to track their activities across the web.[106] Although much of this information is anonymous in the narrow sense of not including a user's name, profiling data may include both personally identifiable information (PII) and non-personally identifiable information (non-PII).[107] This data may also be "combined with 'demographic' and 'psychographic' data from third-party sources, data on the consumer's offline purchases, or information collected directly from consumers through surveys and registration forms."[108] The resulting profiles often are

---

[106] *See* FED. TRADE COMM'N, ONLINE PROFILING: A REPORT TO CONGRESS 1–3 (2000), *available at* http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf [hereinafter ONLINE PROFILING: A REPORT TO CONGRESS].

[107] *Id.* at 3–4. PII is data that can be linked to specific individuals such as name, address, phone number, e-mail address, social security number, and driver's license number. Non-PII consists mainly in page views, search query terms, purchases, and click-through responses to ads. Although network advertisers link the profiles that result from tracking such consumer activity to a unique identifier, they generally do not know the name of a specific consumer. Hence, profiles are considered "anonymous." *But see* STAFF REPORT ON SELF-REGULATORY PRINCIPLES, *supra* note 40, at 21–22 (rejecting this distinction because "the traditional notion of what constitutes PII versus non-PII is becoming less and less meaningful and should not, by itself, determine the protections provided for consumer data").

[108] *Id.* at 5.

highly detailed and revealing yet remain largely invisible to consumers, many of whom react negatively when informed that their online activities are monitored.[109]

The FTC recognized several benefits in the use of cookies and other technologies to create targeted ads, such as providing information about products and services in which consumers are interested and reducing the number of unwanted ads. More importantly, targeted ads increase advertising revenues, which subsidize free online content and services.[110] On the other hand, the FTC acknowledged several major privacy concerns raised by online profiling such as the lack of consumer awareness; the scope of the monitoring activities, which occurs across multiple websites for an indefinite period of time; the potential for associating anonymous profiles with particular individuals; and the risk of companies using profiles to engage in price discrimination.[111] Despite these concerns, the Commission, in June 2000, encouraged the network advertising industry to craft an industry-wide self-regulatory program.[112]

Eight firms responded by announcing the formation of the NAI. Their key tenets included notice to consumers of what information network advertising firms collect and how that information is used, the ability to opt out of receiving tailored ads, and consumer outreach and education.[113] Less than a year later, the NAI completed a

---

[109] *Id.* at 14; *see also* Stephanie Clifford, *Tracked for Ads? Many Americans Say No Thanks*, N.Y. TIMES, Sept. 30, 2009, at B3 (discussing new survey of consumer attitudes to online tracking by advertisers).

[110] *See* ONLINE PROFILING: A REPORT TO CONGRESS, *supra* note 106, at 10; *see also* David S. Evans, *The Online Advertising Industry: Economics, Evolution, and Privacy*, 23 J. ECON. PERSPECTIVES 37 (2009) (noting that although online advertising benefits consumers by increasing the likelihood of their receiving relevant ads and by reducing the costs of advertising to businesses, which may result in lower consumer prices, it also creates a privacy dilemma).

[111] *Id.* at 10–14.

[112] *Id.* at 1.

[113] *See* Daniel Jaye et al., Testimony at the Dep't of Commerce & Fed. Trade Comm'n Public Workshop on Online Profiling: The Role of Self-Regulation (Nov. 8, 1999), *available at* http://www.ftc.gov/bcp/workshops/profiling/comments/nai.htm. By the time this workshop took place, the eight NAI firms faced a highly credible threat of regulatory intervention. Privacy complaints about the use of cookies for advertising purposes were growing and only intensified when DoubleClick announced plans to combine the profiling data it collected online with offline data obtained from a merger with a leading data marketing firm, Abacus. This led to investigations by the FTC and several state Attorneys Generals, a class action consumer lawsuit, Congressional hearings on online profiling, and

voluntary code of conduct that won the FTC's praise and informal endorsement.[114] Under the original NAI Principles, network advertisers engaging in online preference marketing (OPM) are required to offer consumers notice and choice, both of which vary depending on whether the data collected is non-PII or a combination of PII and non-PII.[115] The use of non-PII requires member firms to post on their websites "clear and conspicuous" notice of profiling activities, including what type of data is collected and how it is used; procedures for opting out of such uses; and the retention period for such data.[116] The opportunity to opt-out must be accessible on the firm's or the NAI's website. Moreover, NAI firms that enter into a contract with a publisher for OPM services must require that they offer similar privacy protections to consumers.[117] The merger of PII and non-PII for OPM purposes are subject to substantially similar notice requirements, but the choice options are more complex. Network advertisers merging PII with previously collected non-PII must first obtain a consumer's affirmative (opt-in) consent, whereas mergers of PII and non-PII collected on a going forward basis must afford consumers "robust notice" and an opt-out choice; the latter rule also applies to using PII collected offline when merged with PII collected online.[118] Enforcement is another requirement that applies to

---

massively bad publicity. *See* Evan Hansen, *Double-click Postpones Data Merging Plan,* CNet (Mar. 2, 2000), http://news.cnet.com/DoubleClick-postpones-data-merging-plan/2100-1023_3-237532.html?tag=mnco (last visited July 12, 2011).

[114] *See* FED. TRADE COMM'N, ONLINE PROFILING: RECOMMENDATIONS 9 (July 2000), *available at* http://www.ftc.gov/os/2000/07/onlineprofiling.pdf (praising the NAI for both the "innovative aspects of their proposal" and for adopting self-regulatory principles that "address the privacy concerns consumers have about online profiling and are consistent with fair information practices").

[115] *See* FED. TRADE COMM'N, NETWORK ADVERTISING INITIATIVE: SELF-REGULATORY PRINCIPLES FOR ONLINE PREFERENCE MARKETING BY NETWORK ADVERTISERS 4 (2000), *available at* http://www.ftc.gov/os/2000/07/NAI%207-10%20Final.pdf.

[116] *Id.*

[117] *Id.* at 5. Similar requirements (excluding the opportunity to opt out) apply to the collection of data for ad delivery and reporting purposes. *Id.* at 6–7.

[118] *Id.* at 8. "Robust notice" is defined as "clear and conspicuous notice about the scope of the non-PII that would be made personally identifiable and how the non-PII will be used as a result of such merger." *Id.* at 9. It is not obvious how robust notice differs from ordinary notice, which also must be "clear and conspicuous."

all NAI members,[119] and the NAI offers several additional consumer protections as well.[120]

For the next seven years, the NAI principles remained unchanged until two highly publicized incidents sparked renewed concerns over online profiling practices. The first incident involved a civil subpoena to Google seeking search query records.[121] The second involved disclosure of millions of search queries by AOL.[122] Both incidents involved leading search firms, whose business models are premised on providing free searches and a host of related services in exchange for serving targeted ads to customers based on their search queries and other data collected from users of these services. Over the next two years, consumer privacy organizations began filing complaints regarding online advertising practices and the proposed mergers between industry giants such as Google and DoubleClick. Both E.U. data protection agencies and the FTC started reviewing these activities, while the industry responded to the regulatory pressure by proposing new practices and technologies for improving search

---

[119] The NAI Principles offer two options: (1) participation in a seal program that includes "typical" elements such as random third-party audits, a complaint process, and sanctions including revocation of the seal accompanied by public notice, or (2) independent audits of a member's practices that would be made publicly available on the NAI's website. *Id.* at 12.

[120] These include a prohibition on the use of "sensitive data" (defined as PII about "sensitive medical or financial data, sexual behavior or sexual orientation, [and] social security numbers") for OPM purposes; an opt-in requirement for using any previously collected data (non-PII or PII) under a materially different privacy policy; a set of rather limited pledges regarding security and access; and an agreement by NAI members to abide by the principles of notice, choice, access and security as defined by the OPA Guidelines. *Id.* at 3, 6.

[121] The Dept. of Justice (DOJ) sought these records to assist the U.S. government in proving the constitutionality of the Child Online Protection Act. *See* Verne Kopytoff, *Google Says No to Data Demand: Government Wants Records of Searches*, S.F. CHRON., Jan. 20, 2006, at A1. A district court eventually approved a narrower DOJ request requiring Google to turn over a random sample of 50,000 URLs for use in the DOJ study. *See* Gonzalez v. Google, 234 F.R.D. 674 (N.D. Cal. 2006).

[122] This occurred the following year, when AOL inadvertently disclosed about 20 million search queries with random identifiers in lieu of user ID's, but the queries were sufficiently revealing to allow reporters to identify an individual user by name. Press coverage of both incidents suggest that consumers were very surprised to learn that Google retained search records at all and could be forced to hand them over to the government, or that AOL would voluntarily share such records with researchers. *See* Michael Barbaro & Tom Zeller Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, at A1.

privacy and addressing online profiling practices.[123] Then, in 2007, the FTC held a two-day workshop focused on behavioral targeting. In connection with this workshop, the World Privacy Forum (WPF) prepared a highly critical report attacking the effectiveness of the NAI's self-regulatory scheme during the previous seven years.[124] NAI responded to these and other criticisms by releasing a draft update to its original NAI Principles (this time soliciting public comments on the proposed changes).[125] The newly expanded organization[126] then published its revised code of conduct to mixed reviews.

Clearly, the NAI Principles constitute a voluntary code of conduct, exhibiting virtually all of the relevant characteristics as described in Part II.A. As such, do the original (or revised) NAI principles suffer from the shortcomings associated with voluntary codes, or do they live up to their promise of protecting consumer privacy? In other words, how do the principles fare when assessed against the six elements of the normative framework described in Part II.C?

To begin with, the principles are efficient for member firms, but less so for government (given the ongoing costs of FTC oversight) and for the public (given the negative externalities associated with behavioral profiling).[127] Second, when the original principles were

---

[123] *See* Kevin J. O'Brien & Thomas Crampton, *European Union Probes Google Over Data Retention Policy*, N.Y. TIMES, May 26, 2007, at C3.

[124] *See* PAM DIXON, THE NETWORK ADVERTISING INITIATIVE: FAILING AT CONSUMER PROTECTION AND SELF-REGULATION 14-27, 28-30 & 32-38 (2007), *available at* http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf [hereinafter WPF Study] (arguing that the NAI opt-out mechanism was a failure because it often didn't work; consumers sometimes deleted the opt-out cookie inadvertently, and this technology was ineffective against newer tracking technologies; that there was a severe and rapid drop-off in NAI membership from twelve members in 2000 to just two members in 2003, although this may have been due in part to the dot.com collapse; and raising doubts about NAI's compliance program, which had been outsourced to Truste, for having a weak consumer complaint mechanism and for neglecting random audits).

[125] *See* Network Advertising Initiative, NAI Principles 2008: The Network Advertising Initiative's Self-Regulatory Code of Conduct for Online Behavioral Advertising (2008), *available at* http://networkadvertising.org/networks/NAI_Principles_2008_Draft_for_Public.pdf.

[126] *See* NETWORK ADVERTISING INITIATIVE, NAI'S SELF-REGULATORY CODE OF CONDUCT (2008), *available at* http://www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf (in the wake of renewed public scrutiny, the NAI grew to twenty-five members).

[127] *See* Evans, *supra* note 110, at 33 (noting the privacy externalities of overly lenient regulation of online ads). As Evans states: "Consumers could incur the costs of having

issued in 2000, privacy advocates complained about the NAI's lack of transparency. Although the principles were posted online, the preliminary discussions between the NAI firms and the FTC were far less transparent—they took place largely behind closed doors.[128] Third, the original principles were considered weak on notice, choice, and access;[129] and critics were not much happier with the retrograde forms of notice, choice, and access permitted under the 2009 revised Principles.[130] Fourth, at least in the early years, network advertising firms suffered from both versions of the free rider problem (feigned compliance and non-participation) and the NAI program did not include any mechanisms that capably addressed them.[131] It remains to

---

private information disclosed and potentially misused, and incur the costs of reducing their use of the web because of concerns over privacy. Regardless of whether their private information is disclosed consumers may not like receiving ads that reflect too much knowledge about them even if it is only a software program on a remote server that has that knowledge."

[128] *See* EPIC.org, Network Advertising Initiative: Principles Not Privacy, http://epic.org/privacy/Internet/nai_analysis.html (noting that privacy and consumer groups were all but excluded from the NAI-FTC discussions with the exception of a single meeting very late in the process). In revising the principles in 2009, however, NAI took a very different approach. It not only published draft principles for public comment, but then issued revised principles and simultaneously published a fifty-page summary of these comments along with its own responses, which in many cases consisted in changing the draft principles. *See* NETWORK ADVERTISING INITIATIVE, RESPONSE TO PUBLIC COMMENTS RECEIVED ON THE 2008 NAI PRINCIPLES DRAFT (2008), *available at* http://www.networkadvertising.org/networks/NAI%20Response%20to%20Public%20Comments_Final%20for%20Website.pdf. Of course, NAI, not the government, still holds the pen and makes final decisions on how to balance public comments against industry goals.

[129] *See* WPF Study, *supra* note 124 *passim*.

[130] Although the FTC applauded the 2009 revisions for extending the scope of the access and security principles to data used not only for behavioral targeting, but also for practices such as ad delivery and reporting on a single domain or across multiple domains site (so-called "multi-site advertising"), the Commission also criticized NAI's failure to develop more effective and innovative disclosure and choice options beyond the mere inclusion in the text of a posted privacy policy. *See* STAFF REPORT ON SELF-REGULATORY PRINCIPLES, *supra* note 40, at 14.

[131] As the WPF study observed, the FTC was unsuccessful in maintaining a serious threat of government regulation, and NAI membership rapidly deteriorated once Muris announced his new agenda and Congress failed to enact privacy legislation. Moreover, by creating a category for "Associate Members" (who were not required to abide by the NAI Principles), NAI institutionalized the problem of half-hearted participation. *See* WPF Study, *supra* note 124, at 28-31. This improved only after the FTC showed renewed interest in behavioral advertising, and advocacy groups began filing complaints with the Commission objecting both to the profiling practices of network advertising and search firms, and to proposed mergers involving the leading players.

be seen whether these issues will persist now that the FTC is again encouraging self-regulation, although current policy may change depending on whether or not Congress enacts new privacy legislation. Fifth, the NAI program is also deficient with respect to all three oversight and enforcement criteria identified in the DOC study referred to above. In terms of consumer recourse, the NAI Principles make formal provision for consumers to file complaints (which are now handled in-house) but are silent on remedies.[132] As to verification and consequences for failure to comply, the NAI track record is extremely poor both on auditing compliance and invoking remedies (such as revocation, public suspension of membership, and referral to the FTC). Indeed, it is not clear whether such actions have occurred during its previous nine years of operation, although NAI's approach to audits seems to be changing for the better.[133] Finally, although the more open process NAI used in revising its principles in 2009 is a good first step towards using second-generation strategies, it is still deficient in terms of direct negotiations, Coasian bargaining, and mutual buy-in.

B. THE U.S.-E.U. SAFE HARBOR AGREEMENT

Article 25 of the European Union Data Protection Directive (E.U. Directive) limits the transfer of personal data to a third country unless it provides an "adequate" level of privacy protection.[134] Unlike the E.U. Directive, which is an omnibus statute protecting all personal information of European citizens, U.S. privacy protection relies on a combination of sectoral laws, FTC enforcement powers, and self-regulation. As a result of these differences, U.S. firms were uncertain about the legality of data flows from the E.U. to the U.S. under the

---

[132] Given how little consumers understand about profiling practices, it seems unlikely that they would be able to determine which NAI firm might be misusing their data or whether any violation of the Principles has occurred.

[133] The NAI initially promised random audits by seal programs, but there is no data on whether these ever occurred. Under the NAI's newly announced Compliance Program, NAI staff conducted its first annual compliance reviews of member companies and posted a summary of the results on the website. *See* NETWORK ADVERTISING INITIATIVE, 2009 ANNUAL COMPLIANCE REPORT (2009), *available at* http://www.networkadvertising.org/pdfs/2009_NAI_Compliance_Report_12-30-09.pdf (summarizing the annual review by NAI Staff of member companies' compliance with the new NAI Principles).

[134] Council Directive 95/46, art. 25(1), 1995 O.J. (L 281) 31 [hereinafter Council Directive 95/46/EC].

Article 25 adequacy standard. After several years of discussion, the European Commission (EC) and the DOC entered into a Safe Harbor Agreement (SHA) spelling out Privacy Principles that would apply to U.S. companies and other organizations receiving personal data from the E.U.[135]

The SHA creates a voluntary mechanism enabling U.S. organizations to demonstrate their compliance with the E.U. Directive for purposes of data transfers from the E.U. They must self-certify to the DOC that they adhere to the Privacy Principles that mirror the core requirements of the E.U. Directive (i.e., notice, choice, onward transfer, security, data integrity, access, and enforcement), and repeat this assertion in their posted privacy policy.[136] Although the FTC has agreed to treat any violation of the Privacy Principles as an unfair or deceptive practice, the SHA also defines the mechanism that firms should use to ensure compliance with these principles. These include: (1) readily available and affordable independent recourse mechanisms for investigating and resolving individual complaints and disputes;[137] (2) verification procedures regarding the attestations and assertions businesses make about their privacy practices, which may include self-assessments (which must be signed by a corporate officer and made available upon request) *or* outside compliance reviews;[138] and (3) remedies for failure to comply with the Privacy Principles, including not only correction of any problems, but also various sanctions such as publicizing violations, suspension, removal from a seal program, and compensation for any harm caused by the violation.[139] Truste,

---

[135] On July 21, 2000, the DOC formally issued the Safe Harbor Privacy Principles and other supplementary documents explaining how U.S. enforcement mechanisms would apply, and addressing related issues of interpretation, with the understanding that the Commission would then determine that this safe harbor framework provides adequate protection for the purpose of data transfer to participating companies. *See* DEP'T OF COMMERCE, SAFE HARBOR PRIVACY PRINCIPLES (2000), *available at* http://www.ita.doc.gov/td/ecom/SHPRINCIPLESFINAL.htm.

[136] Note that there are other ways of meeting the adequacy requirement, such as individual consent, standard contractual clauses, binding corporate rules, and approved codes of conduct.

[137] *See* Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666, 45,673-74 (July 24, 2000).

[138] *Id.* at 45,670-71.

[139] *Id.* at 45,673-74. Note that the SHA permits (but does not require) compensation to individuals for losses incurred as a result of non-compliance.

BBBOnline, and several other self-regulatory privacy programs already in operation when the SHA took effect then developed Safe Harbor programs specifically designed to satisfy (1) and (3). The verification requirement is satisfied by self-assessment or third-party compliance reviews.

The SHA has been described as an "uneasy compromise" between the comprehensive regulatory approach of the E.U. and the self-regulatory approach preferred by the U.S.[140] This partly reflects the fact that in providing the Privacy Principles and related documents that form the SHA, the DOC lacked any direct statutory authority to regulate online privacy and therefore had to rely solely on its enabling statute, which only grants authority to foster, promote, and develop international commerce. Applying Priest's typology, it is clear that SHA seal programs more closely resemble regulatory self-management programs than voluntary codes of conduct. One might expect, therefore, that such programs would fare better than NAI in demonstrating greater transparency, fewer free rider issues, better coverage, and meaningful oversight and enforcement.[141] Unfortunately, this is not borne out by the available evidence.[142]

First, as a government initiative, the SHA Privacy Principles are highly transparent, at least in terms of DOC announcing the relevant standards that industry would need to follow. But second, as noted below, virtually no information is available regarding the performance of firms in terms of these standards. Third, SHA seal programs fare better than NAI in terms of formulating program guidelines that—at least in theory—adhere to all of the Privacy Principles. However, both the E.U. Study and the Galexia Study found that a high percentage of

---

[140] *See* Chris Connolly, *The US Safe Harbor - Fact or Fiction?*, 96 PRIVACY L. AND BUS. INT'L 1, 4 (2008).

[141] *See* Damon Greer, The U.S.-E.U. Safe Harbor Framework, Presentation at the Conference on Cross-Border Data Flows, Data Protection, and Privacy (2007), *available at* http://www.SafeHarbor.governmentools.us/documents/1A_DOC_Greer.ppt (suggesting that DOC considers the SHA privacy framework a success).

[142] The following analysis relies on (1) a 2004 report, prepared at the request of the EC and based primarily on a survey of publicly available privacy policies of participating U.S. companies; *see* JAN DHONT, ET. AL., SAFE HARBOUR AGREEMENT IMPLEMENTATION STUDY 105-07 (2004), *available at* http://ec.europa.eu/justice/policies/privacy/docs/studies/safe-harbour-2004_en.pdf [hereinafter the EC Study]; and (2) a 2008 report by a British management consulting firm called Galexia, which performed its own study based on the approximately 1,600 firms then listed on the Safe Harbor List. For a summary of the results, *see* Connolly, *supra* note 140 [hereinafter the Galexia Study].

participating firms did not incorporate all seven of the agreed upon Privacy Principles in their own posted privacy policies.[143] Fourth, the SHA, like the NAI agreement, also suffers from both versions of the free rider problem—many firms self-certify their adherence to the Privacy Principles without even revising their posted privacy policies in accordance with SHA requirements and, even if one excludes firms that rely on alternative methods for demonstrating adequacy, the roughly 2,000 participants on the DOC's Safe Harbor List represent only a tiny fraction of firms that transfer data from the E.U. to the U.S. Fifth, as to oversight and enforcement, the E.C. Study noted that *no* complaints have been received and handled "despite frequent and even flagrant inconsistencies and violations in implementation,"[144] while according to the Galexia Study, fewer than one in four companies registered for safe harbor were in compliance with the Enforcement Principle and even fewer offered an affordable dispute resolution process.[145] Indeed, it was not until the summer of 2009 that the FTC announced its *first* enforcement action against a U.S. company for violation of the SHA.[146]

The SHA allows firms to meet the verification requirements of the Enforcement Principle either through self-assessment *or* outside

---

[143] *See* EC Study, *id.* (finding inadequate representation of various Privacy Principles, misrepresentation of company memberships in self-regulatory programs, safe harbor programs that did not incorporate all of the Privacy Principles, and weak implementation of the Enforcement Principle); *see also* the Galexia Study, *id.* (finding that relatively few participants published privacy policies reflecting all of the Principles as required by the SHA; that a large number of firms failed to provide an independent recourse mechanism or selected a mechanism that was not affordable, such as arbitration; and that many firms claimed to be participants and continue to be accredited by self-regulatory SHA programs even though they no longer appeared on the Safe Harbor List maintained by the DOC).

[144] EC Study, *id.* at 107-08.

[145] Galexia Study, *supra* note 140, at 7.

[146] *See* Press Release, Fed. Trade Comm'n, Court Halts U.S. Internet Seller Deceptively Posing as U.K. Home Electronics Site (August 6, 2009), *available at* http://ftc.gov/opa/2009/08/bestpriced.shtm (the FTC brought suit against a California company for falsely claiming, in its privacy policy, that it was certified under the SHA when in fact it was not). A few months later, the FTC announced proposed settlements in six more false claims cases, suggesting that the Commission is stepping up its Safe Harbor enforcement activity. *See* Press Release, Fed. Trade Comm'n, FTC Settles with Six Companies Claiming to Comply with International Privacy Framework (October 6, 2009), *available at* http://www.ftc.gov/opa/2009/10/safeharbor.shtm. This near absence of SHA enforcement over the past eight years exacerbates the free rider problems since firms that sign up for SHA and merely feign compliance or refuse to comply are unlikely to suffer any adverse consequences.

compliance reviews. Under the former, the firm must have in place "internal procedures for periodically conducting objective reviews" and must retain any relevant records. They must make the records available upon request in the context of an investigation or a complaint, but have no obligation to share this information with third parties. The same record-keeping requirement applies in the case of outside reviews subject to the same limitation. Thus, both internal and external compliance reviews remain opaque, making it difficult to draw any firm conclusions.[147] Finally, while the SHA in theory fits neatly under Priest's regulatory self-management category, in practice it more closely resembles a voluntary code of conduct given the lack of accountability to government, the free rider problems, the lax monitoring of compliance by seal programs and government agencies, and until quite recently, the absence of enforcement actions or sanctions. In short, it displays none of the characteristics defining second-generation strategies.

C. THE COPPA SAFE HARBOR

Congress enacted the Children's Online Privacy Protection Act of 1998 (COPPA) to prohibit unfair or deceptive acts or practices in connection with the collection, use, or disclosure of personal information from and about children on the Internet. The statute[148] and Final Rule[149] require operators of websites directed at children and of general audience websites with actual knowledge that a user is a child to meet five requirements: (1) notice; (2) parental consent prior to the collection, use, and/or disclosure of personal information from a child; (3) a right of parental review of such information; (4) proportionality; and (5) reasonable security policies.[150]

---

[147] Although the DOC maintains a searchable online list of organizations that adhere to the SHA principles and their certification and compliance status, it is not clear whether a listing of "not current" under certification status has any enforcement implications. *See* Dep't of Commerce, Safe Harbor List, *available at* https://safeharbor.export.gov/list.aspx (showing that almost 2,500 organizations have self-certified, but that many of the listed firms are shown as "non-current" under certification status).

[148] Children's Online Privacy Protection Act of 1998 (COPPA), Pub. L. No. 105-277, § 1302, 112 Stat. 2681-728 (codified at 15 U.S.C. §§ 6501-06).

[149] Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888 (Nov. 3, 1999) (codified at 16 C.F.R. pt. 312) [hereinafter COPPA Final Rule].

[150] *See* COPPA, 15 U.S.C. § 6502 (2006); *see also* 16 C.F.R. § 312.3(a)-(e).

COPPA provides both federal and state enforcement mechanisms and penalties against operators who violate the provisions of the implementing regulations.[151] The statute by its terms also establishes an optional safe harbor program as an alternative means of compliance for operators that follow self-regulatory guidelines, which must be approved by the FTC under a notice and comment procedure.[152] There are three key criteria for safe harbor approval. Self-regulatory guidelines must (1) meet or exceed the five statutory requirements identified above; (2) include an "effective, mandatory mechanism for the independent assessment of . . . compliance with the guidelines" such as random or periodic review of privacy practices conducted by a seal program or third-party; and (3) contain "effective incentives" to ensure compliance with the guidelines such as mandatory public reporting of disciplinary actions, consumer redress, voluntary payments to the government, or referral of violators to the FTC.[153]

The avowed purpose of the COPPA safe harbor is to facilitate industry self-regulation, and it does so in two ways. First, operators that comply with approved self-regulatory guidelines are "deemed to be in compliance" with all regulatory requirements.[154] To benefit from safe harbor treatment, operators need not individually apply for approval as long as they fully comply with approved guidelines that are applicable to their business. According to the COPPA Final Rule, such compliance serves "as a safe harbor in any enforcement action" under COPPA unless the guidelines were approved based on false or incomplete information.[155] Second, the safe harbor allows "flexibility

---

[151] *See* COPPA, 15 U.S.C. §§ 6502(c) and 6504 (2006). In April 2002, the FTC conducted a survey of the information collection practices of 144 children's websites and found that the general trend of the sites is one of increased compliance, even though some COPPA provisions, such as requirements about specific disclosures, have been followed less consistently. *See* FED. TRADE COMM'N, PROTECTING CHILDREN'S PRIVACY UNDER COPPA: A SURVEY ON COMPLIANCE (2002), *available at* http://www.ftc.gov/os/2002/04/coppasurvey.pdf. The Commission has also settled fifteen cases for violations of the COPPA Rule, including two that each resulted in civil penalties of $1 million. *See* Fed. Trade Commission, Privacy Initiatives, http://www.ftc.gov/privacy/privacyinitiatives/childrens_enf.html (last visited Mar. 14, 2011).

[152] COPPA, 15 U.S.C. § 6503 (2006); *see generally* 16 C.F.R. § 312.10.

[153] 16 C.F.R. § 312.10(b)(2).

[154] COPPA, 15 U.S.C. § 6503(b)(2)(2006).

[155] COPPA Final Rule, *supra* note 149, at 59, 906.

in the development of self-regulatory guidelines" in a manner that "takes into account industry-specific concerns and technological developments."[156] Industry groups interested in providing safe harbors must submit their self-regulatory guidelines to the FTC for approval.[157] To date, the FTC has reviewed six safe harbor programs and approved four of them. With all of the approved safe harbor programs satisfying the three criteria set out in the preceding paragraph, the COPPA safe harbor exemplifies Priest's regulatory self-management category insofar as the statue sets regulatory policy and rules but assigns program sponsors the responsibility for drafting self-regulatory guidelines, implementing and operating the program, and enforcement. A brief assessment of CARU's monitoring and complaint-handling system shows the success of the safe harbor program from an enforcement standpoint.[158]

Between 2000 and 2008, CARU reported on almost 200 cases; a few originated in consumer complaints and the rest resulted from CARU's routine monitoring of any website that may be reasonably expected to attract children or teen users.[159] Issues ranged from inadequate privacy policies to the lack of a neutral age-screening process to collection or disclosure of PII from children without parental consent. The companies resolved all of the cases in question by agreeing to change their practices as directed by CARU. In

---

[156] *Id.* According to the FTC, self-regulatory programs are desirable because they "often can respond more quickly and flexibly than traditional statutory regulation to consumer needs, industry needs and a dynamic marketplace." *See* FED. TRADE COMM'N, IMPLEMENTING THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT: A FEDERAL TRADE COMM'N REPORT TO CONGRESS (2007) 22-23, *available at* http://www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf [hereinafter FTC COPPA REPORT].

[157] *See* 16 C.F.R. § 312.10(c)(1)-(2) (providing that the FTC will then act on the application within 180 days of the filing, and after the proposed guidelines have been subject to notice and comment).

[158] CARU was established in 1974 by the National Advertising Division (NAD) of the Council of Better Business Bureaus. Because the NAD maintains a publicly available archive of case reports of all formally opened cases involving a website's failure to comply voluntarily with the CARU guidelines, it is possible to evaluate CARU's track record of compliance. The case reports are available upon request. *See* National Advertising Division, Case Reports and Procedures, http://www.nadreview.org/search/search.aspx?doctype=1&casetype=2 (last visited Mar. 14, 2011).

[159] All four approved safe harbor programs periodically monitor their member websites, whereas CARU also monitors non-member websites.

addition, CARU referred one case to the FTC that resulted in a $400,000 settlement.[160] In a second case, the respondent entered into a consent decree with the FTC that included signing up for the CARU safe harbor.[161] And in a third case, the FTC initiated a COPPA lawsuit based in part on CARU's determination of compliance shortcomings.[162] This is an impressive record considering that since 2000, the FTC has brought a total of only fifteen COPPA enforcement cases. In short, CARU's compliance review and disciplinary procedures clearly have been successful in complementing the FTC's enforcement of COPPA, due in no small measure to its policy of engaging in widespread monitoring of child-oriented websites as opposed to members' sites only. This, in turn, allows the Commission to focus its resources on higher profile matters.[163]

How well do COPPA safe harbor programs (and CARU, in particular) fare when evaluated against the now familiar normative criteria? Clearly, CARU harnesses industry expertise, but probably costs more to operate than the NAI or SHA seal programs given its extensive enforcement activities. Second, like the SHA, COPPA is very strong on producing and reporting information regarding relevant legal standards but weak on performance data.[164] Third, as compared to both the NAI and SHA, only the COPPA safe harbor programs achieve full coverage of substantive privacy requirements as might be expected given the FTC's mandatory review of program guidelines, all of which must offer principles that "meet or exceed" statutory

---

[160] *See* Press Release, Fed. Trade Comm'n, UMG Recordings, Inc. to Pay $400,000 to Settle COPPA Civil Penalty Charges (Sept. 13, 2006), *available at* http://www.ftc.gov/opa/2004/02/bonziumg.shtm.

[161] *See* Press Release, Fed. Trade Comm'n, Imbee.com Settles FTC Charges Social Networking Site for Kids Violated the Children's Online Privacy Protection Act (Jan. 30, 2008), *available at* http://www.ftc.gov/opa/2008/01/imbee.shtm.

[162] *See* Press Release, Fed. Trade Comm'n, Website Targeting Girls Settles FTC Privacy Charges (Oct. 21, 2001), *available at* http://www.ftc.gov/opa/2001/10/lisafrank.shtm.

[163] *See* FTC COPPA REPORT, *supra* note 156, at 23-24.

[164] The COPPA Rule was developed following a notice and comment procedure in which the FTC received 132 comments in response to its Notice of Proposed Rulemaking. The FTC also held a public workshop seeking additional information on the issue of how to obtain parental verification. *See* COPPA Final Rule, *supra* note 149, at 59,888. Although the COPPA Rule requires periodic compliance reviews or other effective assessment mechanisms, it makes no provision for publishing these reviews or any underlying data.

requirements.[165] Fourth, free rider problems are minimal in the COPPA safe harbor program because firms that resist joining an approved program remain subject to the statutory requirements, thereby deriving little competitive advantage from free riding. Additionally, the number of CARU investigations seems high enough to discourage feigned compliance by participating firms, especially given CARU's willingness to refer cases to the Commission, and the FTC's aggressive enforcement stance with respect to children's privacy issues.[166] Fifth, as to oversight and enforcement, COPPA requires that approved safe harbor programs engage in ongoing monitoring of their members' practices to ensure compliance with program guidelines and the participant's own privacy notices. CARU's strong record of investigating compliance issues identified in complaints or as a result of routine monitoring (coupled with FTC's higher profile enforcement actions) rebuts the usual charge that self-regulatory programs are weak on enforcement.[167] To the contrary, the COPPA safe harbor programs, like other well-organized and committed industry groups, "help free up scarce government regulatory resources to address the recalcitrant few rather than the compliant majority."[168] The CARU program stands out both for publishing case reports on non-member compliance issues and for having, in fact, referred several cases to the FTC.

Finally, while the CARU program is far superior to either the NAI or SHA in terms of the preceding five criteria, it lacks many of the attributes of second-generation regulatory strategies. There is no

---

[165] Indeed, as noted above, the COPPA Rule requires that applicants submit a comparison of substantive requirements of the rule with the proposed guidelines and that the FTC act on their request for approval only after subjecting the proposal to a formal notice and comment procedure. This is not to say that every firm that participates in an approved COPPA safe harbor program is in full compliance with the Rule. Rather, the point is that the degree of completeness is directly related to the strength of the government's mandate over the applicable self-regulatory scheme.

[166] *See supra* notes 159-162 and accompanying text.

[167] The monitoring and complaint-handling records of the other three approved safe harbor programs are more difficult to assess given the dearth of public documentation. However, the complaint record of CARU is disappointing. Only a small number of the almost 200 investigations originated with consumer complaints (but all were resolved satisfactorily).

[168] *See* Sinclair, *supra* note 6, at 537; AYERS & BRAITHWAITE, *supra* note 46, at 129 ("A fundamental principle for the allocation of scare regulatory resources ought to be that they are directed away from companies with demonstrably effective self-regulatory systems and concentrated on companies that play fast and loose.").

Coasian bargaining and too little industry buy-in.[169] Moreover, the COPPA regulations are neither very flexible nor do they take into account "industry-specific concerns and technological developments." Although the Commission expressly characterized the assessment mechanisms and compliance incentives described in the Final Rule as "performance standards" that may be satisfied by equally effective alternatives,[170] a review of the self-regulatory guidelines of CARU, Truste, ESRB and Privo shows relatively little differentiation by sector, technology, or innovative methods of assessment or compliance.[171] This is at least partly the result of the safe harbor approval process, which requires a side-by-side comparison of the substantive provisions of the COPPA rule with the corresponding provisions of the guidelines. The reason firms participate in safe harbor programs is probably due less to regulatory flexibility, and more to a desire to share in the brand recognition of the program seal, to develop a closer working relationship with FTC staff, and to draw on the additional expertise of program staff.

*****

---

[169] Indeed, very few firms have signed up for safe harbor programs. CARU has the fewest members (about ten), while Privo has twenty-two, and ESRB and Truste each have about thirty. *See* Email from Joanne Furtsch, Senior Privacy Architect, Truste, to Ira Rubinstein, Adjunct Professor of Law, New York University School of Law (Sept. 17, 2009) (on file with author); Telephone Interview with Phyllis B. Spaeth, Associate Director, CARU (Sept. 23, 2009); Telephone interview with Dona J. Fraser, Director, Privacy Online, ESRB (Sept. 28, 2009); Email from Stephen Kline, Vice President, Public Affairs, Privo, to Ira Rubinstein (Sept. 29, 2009) (on file with author). All told, fewer than 100 firms have been certified under approved safe harbor programs (although some of the ESRB and Truste certifications cover multiple websites). The most likely explanation for this low rate of participation is that deemed compliance is not a strong enough incentive to persuade firms to bear the costs of joining a safe harbor program and abiding by its guidelines when they have to comply with all but identical statutory requirements in any case. Moreover, the COPPA Rule permits a firm to claim safe harbor benefits even though it has not joined a program, but instead relies on internal processes for compliance and enforcement.

[170] COPPA Final Rule, *supra* note 149 at 59,906-07 (stating that required assessment mechanisms and compliance incentives are not considered as mandatory practices, but rather as "performance standards," and that the listed methods are only "suggested means for meeting these standards").

[171] Although ESRB is a trade association for the gaming industry and draws all of its members from this sector, this is not reflected in any differences between its guidelines and those of the other three COPPA safe harbor programs. In addition, although Privo is unique in offering its own turnkey identity solution, which handles children's registration and parental consent under COPPA, this seems more like a business decision than a direct response to COPPA's "flexible" regulations.

The three preceding case studies all describe well-established self-regulatory programs and evaluates them against five public policy criteria and a sixth criteria focusing on second-generation regulatory strategies. This next section is different. It explores a few overseas cases of privacy covenants under law and then hones in on a very recent case in which U.S. firms, when threatened with prescriptive regulation, chose to engage in a multi-stakeholder process (known as the Global Network Initiative or GNI) to define privacy and free speech principles for the Internet. While it is too soon to assess the GNI against the public policy criteria, and while the GNI might fare poorly in operational terms when compared to a statutory safe harbor such as CARU, the GNI nevertheless points the way to the use of mutually self-interested bargaining to achieve superior performance by good actors.

D. PRIVACY COVENANTS

In his article discussing innovative environmental privacy tools, Hirsch's primary examples of a privacy covenant are the Dutch codes of conduct. Dutch data protection law (which is a comprehensive statute implementing the E.U. Data Directive) allows industry sectors to draw up codes for processing of personal data, which are then submitted to the Dutch Data Protection Authority (DPA) for review and approval.[172] Specifically, organizations considered "sufficiently representative" of a sector and that are planning to draw up a code of conduct may ask the DPA for a declaration that "given the particular features of the sector or sectors of society in which these organizations are operating, the rules contained in the said code properly implement" Dutch law.[173] Article 25(4) of the PDPA further provides that such declarations shall be "deemed to be the equivalent to" a binding administrative decision, making it similar in effect to FTC approval of COPPA safe harbor guidelines. According to Hirsch, the DPA has approved at least twelve such codes covering various industry sectors, each with its own tailored compliance plan that is nevertheless consistent with the broader requirements of the Dutch data protection law.[174] Outside of Europe, other countries have

---

[172] *See* the Dutch Personal Data Protection Act (PDPA), Chap. 3, Art. 25, *available and translated at* http://www.dutchdpa.nl/downloads_wetten/wbp.pdf.

[173] *Id.*

[174] Hirsch, *supra* note 66, at 54 – 56. This Dutch approach is generally consistent with Article 27(1) of the E.U. Data Directive, which states that "Member States and the

adopted a similar approach to privacy covenants. For example, Australian privacy law also permits organizations to develop sectoral privacy codes for the handling of personal information "designed to allow for flexibility in an organization's approach to privacy," while at the same time guaranteeing consumers "that their personal information is subject to minimum standards that are enforceable in law."[175] Finally, New Zealand privacy law also treats approved codes of conduct as instruments of law with binding effect.[176]

In the U.S., where comprehensive privacy law is lacking, there is no possibility of firms or industry negotiating privacy covenants with regulators, unless one wants to treat FTC consent decrees as a type of covenant. Thus, the covenanting approach in the U.S. arises only when there is a credible threat of federal privacy regulation and firms sit down with regulators to negotiate a code of conduct in lieu of regulation. In his article, Hirsch cites the OPA Guidelines as an "incomplete" step towards a covenanting approach, and gives three

---

Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors." *See* Council Directive 95/46/EC, *supra* note 134, at Article 27(1). Like the Netherlands, Ireland also has approved several codes of practices under its data protection law. *See* Irish Data Protection Commissioner, Self-Regulation and Codes of Practice, http://www.dataprotection.ie/viewdoc.asp?DocID=98 (last visited Feb. 3, 2011).

[175] *See* OFFICE OF THE FEDERAL PRIVACY COMMISSIONER, GUIDELINES ON PRIVACY CODE DEVELOPMENT 16 (2001) [hereinafter Code Guidelines], *available at* http://www.privacy.gov.au/materials/types/download/8634/6482. The relevant sections of the Australian Privacy Act of 1988 impose detailed requirements that a privacy code must satisfy to obtain approval. In particular, a code must incorporate all of the relevant National Privacy Principles (NPPs, the Australian version of FIPPs) or set forth obligations that are "at least the equivalent of" the NPPs; specify the organizations to which NPPs apply; and permit organizations to develop their own complaint-handling procedures, such as appointing the Privacy Commissioner or a third party as an independent adjudicator to whom complaints may be made. *See* Privacy Act of 1988, No. 119 §§ 18BB(2)-(3) (1988) (Austrl.). In addition, the Privacy Commissioner must be satisfied "that members of the public have been given an adequate opportunity to comment on a draft of the code." *Id.* at § 18BB(2)(f). The Code Guidelines describe the public consultation requirement in greater detail. Code proponents are required to submit a statement showing that they allowed at least six weeks for consultation and describing who is affected by the code, efforts to consult with affected groups, changes to the proposed code, a summary of any issues that remain unresolved and why, and a list of organizations likely to adopt the code. *See* Code Guidelines at 5–6. Although codes are voluntary, approved codes are legally binding on any company that consents to be bound. *See* § 16A.

[176] *See* Privacy Act of 1993, No. 28 § 46 (1993) (N.Z.).

reasons for this incompleteness.[177] A more recent and telling example of a privacy covenant came about when three leading Internet firms were accused of Internet censorship in China, resulting in a very public controversy and threatened legislation.

In the winter of 2006, Yahoo!, Google and Microsoft had to contend with highly unfavorable publicity and Congressional hearings over their controversial roles in cooperating with Chinese government efforts to monitor and censor the Internet and persecute dissidents.[178] A few months later, Rep. Chris Smith introduced a bill that would have rendered such practices illegal and forced U.S. companies to confront a Hobson's choice: disregard restrictive Chinese licensing requirements imposed on foreign companies as a condition of providing Internet services in the Chinese market or obey Chinese censorship rules in violation of U.S. law.[179] The companies then sat down with a cross-section of human rights organizations, socially responsible investment firms, and academics, and agreed to work on voluntary guidelines for protecting freedom of expression and privacy on the Internet.[180] After eighteen months of negotiations and defections by several NGOs, the multi-stakeholder group reached agreement and launched the GNI, jointly committing to a set of principles and implementation guidelines as well as an accountability

---

[177] *See* Hirsch, *supra* note 66, at 55 (noting three reasons for this incompleteness: (1) the OPA guidelines were developed unilaterally, rather than in negotiations between the FTC and industry, and privacy advocates were excluded, thereby resulting in weak standards; (2) the FTC threatened but failed to issue prescriptive regulations, exacerbating free rider problems; and (3) absent new legislation, the FTC gained no additional powers to enforce the OPA guidelines).

[178] Tom M. Zeller, Jr., *Internet Firms Facing Questions about Censoring Internet Searches in China*, N.Y. TIMES, Feb. 15, 2006, at C3. For a more detailed description of the incidents involving each company, *see* HUMAN RIGHTS WATCH, RACE TO THE BOTTOM: CORPORATE COMPLICITY IN CHINESE INTERNET CENSORSHIP (2006), *available at* http://china.hrw.org/timeline/2006/race_to_the_bottom.

[179] Carrie Kirby, *Chinese Internet vs. Free speech: Hard Choices for US Tech Giants*, S.F. CHRONICLE, Sept. 18, 2005, at A1.

[180] Other stakeholders included the Center for Democracy and Technology, the Electronic Frontier Foundation, Human Rights First, Human Rights in China, Human Rights Watch, the Calvert Group, Domini Social Investments, and F & C Asset Management. For a full list of participants, *see* Participants, http://www.globalnetworkinitiative.org/participants/index.php (last visited Mar. 14, 2011).

system based on independent, third-party assessments.[181] More recently, a GNI member (Google) announced that it would shut down its Chinese search engine rather than continuing to censor the results,[182] and began automatically redirecting Chinese customers to an uncensored version of Google search hosted in Hong Kong.[183]

Why did Yahoo!, Google, and Microsoft agree to participate in a multi-stakeholder process in which a successful outcome required convening a group of actors with divergent interests (often at loggerheads with each other), engaging in difficult and protracted negotiations, and staying at the table until a consensus was forged? As described above, the GNI negotiations were an entirely voluntary effort, with no legal mandate as to process or substance. Rather, the parties proceeded on an ad hoc basis and agreed to principles that, while based on international human rights instruments, were not subject to any formal approval criteria or government oversight. Although the U.S. State Department welcomed the GNI initiative, it did not participate in any stakeholder meetings. Cynics may say that the three firms were merely responding to a public relations crisis related to their business operations in China, which forced them to pursue a covenanting approach not only to improve their public image, but to restore public faith in their company integrity and

---

[181] The guidelines state that companies should establish human rights risk assessment procedures and integrate the findings into business decision-making; require that governments follow established domestic legal processes when they are seeking to restrict freedom of expression and privacy; provide users with clear, prominent and timely notice when access to specific content has been removed or blocked; encourage governments, international organizations, and entities to call attention to the worst cases of infringement on the human rights of freedom of expression and privacy; and utilize independent assessments of company implementation of the GNI principles. For the GNI's three core commitment documents, *see* Global Network Initiative, http://www.globalnetworkinitiative.org/index.php (last visited Feb. 3, 2011). Other examples of multi-stakeholder processes designed to achieve basic human rights include the Fair Labor Association Workplace Code of Conduct, the Equator Principles, the Voluntary Principles on Security and Human Rights, and the Extractive Industries Transparency Initiative.

[182] *See* Kim Zetter, *Google to Stop Censoring Search Results in China After Hack Attack*, Wired (Jan. 12, 2010), http://www.wired.com/threatlevel/2010/01/google-censorship-china/ (last visited July 12, 2011).

[183] *See* David Barboza & Miguel Heft, *A Compromise Allows Both China and Google to Claim a Victory*, N.Y. TIMES, July 9, 2010, at B1 (describing how the Chinese authorities agreed to re-issue Google's license for operating a Chinese search service with a website that also contains a link to the uncensored version in Hong Kong).

mollify Congressional demands for government intervention.[184] But even if GNI was initially spurred by negative publicity and a threat of government intervention, it represents a moderately successfully example of the covenanting approach at work.

Granted, negotiating the GNI covenants required a large investment of time and resources by member firms (although perhaps less than might have been required if Congress enacted the Smith bill).[185] On the other hand, the GNI standards are highly transparent and over time its accountability process will require both independent assessments and annual Board reports evaluating each participating company's compliance with the robust set of GNI Principles.[186] With only three members, GNI suffers from severe free rider issues and it is premature to comment on its oversight and enforcement record. In short, GNI is not yet operating at the level of a statutory safe harbor such as CARU. Yet GNI has already delivered on the promise of the covenanting approach. For in the absence of a government-supervised rulemaking process, the stakeholders relied on Coasian bargaining principles—sharing credible information, developing trust based on discussion of common interests, and staying at the bargaining table for as long as necessary—to reach a voluntary agreement and establish a fledgling organization to carry out its terms.

*****

In sum, the preceding case studies have shown that the forms of self-regulation in which government plays an increasingly larger role are more likely to achieve regulatory success than purely voluntary codes of conduct. In particular, a statutory safe harbor outperforms a voluntary code such as the NAI, and a partially mandated approach such as the SHA, across all five of the public policy criteria. This is especially true as to completeness, lack of free rider problems, and, in

---

[184] *See* Neil Gunningham, *Environment, Self-Regulation, and the Chemical Industry: Assessing Responsible Care*, 17 L. & POL'Y 57, 63 (1995) (citing these three factors as the reason that large multinationals in the chemical industry established a voluntary initiative known as Responsible Care in the wake of the Bhopal disaster).

[185] The author has first-hand knowledge of these costs because he was lead privacy counsel at Microsoft until September 2007 and attended the early rounds of GNI negotiations.

[186] *See* GLOBAL NETWORK INITIATIVE, GOVERNANCE, ACCOUNTABILITY, AND LEARNING FRAMEWORK (2008), *available at* http://www.globalnetworkinitiative.org/cms/uploads/1/GNI_-_Governance_Accountability_Learning.pdf.

CARU's case, oversight and enforcement. The review of privacy covenants also highlights a number of subtly different aspects of second-generation strategies. In the case of the GNI, the regulated firms did not seek regulatory flexibility with respect to existing statutes or regulations, but rather to avoid threatened regulation. The talks occurred not at the sectoral level but at the firm level, and in consultation with advocacy groups under a consensus model requiring the approval of all parties based on Coasian bargaining. The resulting principles were not legally binding but seem more than merely precatory given the interest of the participating firms in preserving (or restoring) their reputations for corporate citizenship. Taken together, the set of four case studies suggests that future safe harbor programs need to be overhauled in light of the second-generation strategies illustrated by the GNI experience.

IV. SECOND-GENERATION STRATEGIES FOR PRIVACY REGULATION

Having established the superiority of statutory safe harbors over other forms of self-regulation and the potential of privacy covenants to achieve innovative regulatory solutions, we now turn to three proposed second-generation regulatory strategies. All three leave behind voluntary codes of conduct in favor of privacy covenants in which the government plays a role by defining default requirements and overseeing both implementation and enforcement.

The first is modeled on Hirsch's proposal of a "Project XL" for experimental projects that would enable FTC to test out new, and potentially better, regulatory approaches to privacy and to the adoption of Privacy Enhancing Technologies (PETs). Assuming that Congress enacts a comprehensive privacy law, the Commission could then issue a notice defining the goals, criteria, and requirements of a "Project XL for Privacy" program and invite interested parties to submit proposals for experimental projects.[187] The FTC would then

[187] Of course, in the case of the EPA, environmental statutes and regulations already exist, so Project XL can offer "regulatory flexibility" with respect to these standards in the hopes of achieving superior environmental performance. In the case of the FTC, however, privacy laws do not exist for most industries. Thus, under its existing regulatory authority, the FTC might sponsor an XL-like program only in the context of the Financial Privacy Rule or Safeguards Rule under the Gramm-Leach-Bliley Act of 1999 (GLBA), 15 U.S.C. §§ 6801, 6804, & 6805(b)(2) (2000). But outside the context of the GLBA or a newly enacted comprehensive privacy law, it makes little sense to speak of regulatory flexibility or superior performance with respect to existing standards, which are the hallmarks of Project XL. For a discussion of the FTC's rulemaking authority generally, including whether it has the authority to issue privacy regulations and/or launch a XL-like program under the FTC Act, *see infra* notes 205–209 and accompanying text.

select the best proposals and enter into binding covenants with the sponsors, who would run the projects as experiments subject to agency evaluation and review. Part IV.A describes several innovative ideas of varying scope and ambitiousness that might be suitably recast as XL-like projects. These range from tools and techniques that supplement FIPPs to cutting edge proposals that depart substantially from the familiar control-based system of data protection at the heart of FIPPs.

The second regulatory innovation is simply for the FTC to utilize negotiated rulemaking in appropriate situations. Because negotiated rulemaking presupposes that an agency has rulemaking authority, this approach is limited to those areas where Congress has enacted privacy laws authorizing the Commission to engage in rulemaking under the APA. It seems likely that if Congress enacts privacy legislation, it will grant the FTC authority to promulgate such regulations as may be necessary to carry out the purposes of the new law.[188] Under the NRA, the FTC Chair may then determine if negotiated rulemaking would be in the public interest.[189] Part IV.B will specifically examine what negotiated rulemaking involving behavioral advertising might look like and why it might achieve better results than a rule based on notice and comment.

The third and final approach also requires that Congress enact comprehensive substantive privacy legislation. Thus, Part IV.C assumes that any such law will include a safe harbor provision modeled on § 6503 of COPPA, and sketches out how this safe harbor would work if the incentives for participating and the process for drafting and approving industry guidelines were substantially modified in keeping with second-generation regulatory strategies.

A. PROJECT XL FOR PRIVACY

As discussed in Part II, the ability of consumers to control the collection, use, and transfer of their personal data is a fundamental aspect of any privacy regime centered on FIPPs. The control metaphor assumes that consumers can understand the written privacy policies they encounter online, thereby enabling meaningful consent experiences. But informed consent is rarer than hens' teeth because most online privacy notices are too long and complex, and too laced

---

[188] As is the case with COPPA, *supra* note 148, the Boucher draft, *supra* note 14, at § 8(a)(3), and the Rush bill, *supra* note 15, at § 404.

[189] *See supra* note 92.

with legal jargon, for consumers to understand them. In response, both the private sector and NGOs like the World Wide Web Consortium (W3C) have developed various approaches for improving the notice-and-choice experience. These include point solutions such as use of multilayered notices,[190] standardized table formats for privacy policies,[191] icons representing behavioral advertising practices,[192] experiments with "dashboards" that offer users greater control and transparency over their account data,[193] and improved anonymization techniques that seek to address data retention issues.[194] All of these tools and techniques may be characterized as PETs.[195] In 1997, W3C developed P3P, a computer protocol for helping websites express their privacy practices in a standardized, machine-readable format that could be automatically retrieved and interpreted by tools built into browsers or separate applications. These tools allow end users to set their own privacy preferences and thereby readily

---

[190] *See* THE CENTER FOR INFORMATION POLICY LEADERSHIP, MULTI-LAYERED NOTICES EXPLAINED, http://www.hunton.com/files/tbl_s47Details/FileUpload265/1303/CIPL-APEC_Notices_White_Paper.pdf (last visited Feb. 3, 2011).

[191] *See* P. Kelley, et al., *Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach,* paper presented at CHI '10 Conference, *available at* http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab09014.pdf.

[192] *See Future of Privacy Forum Releases Behavioral Notices Study* (Jan. 27, 2010), http://www.futureofprivacy.org/2010/01/27/future-of-privacy-forum-releases-behavioral-notices-study/ (last visited July 12, 2011) (describing a study of behavioral advertising disclosures using icons as an alternative to providing transparency and choice via traditional online privacy notices).

[193] *See* Miguel Helft, *Google to Offer Ads Based on Interests, With Privacy Rights*, N.Y. TIMES, Mar. 11, 2009, at B3 (describing service that summarizes the data that Google collects from users' accounts).

[194] *See* Miguel Heft, *Yahoo Puts New Limits On Keeping User Data*, N.Y. TIMES, Dec. 18, 2008, at B3 (describing differences in data retention periods among leading search engine providers and quoting a Microsoft spokesman as stating that "the method of anonymization is more important than the anonymization timeframe").

[195] *See* ANNE CAVOUKIAN, & TYLER J. HAMILTON, THE PRIVACY PAYOFF: HOW SUCCESSFUL BUSINESSES BUILD CONSUMER TRUST 252 (2002) (noting that the first use of this term appeared in Privacy-Enhancing Technologies: The Path to Anonymity, a 1995 joint report of the Dutch Data Protection Authority and the Ontario Information Privacy Commissioner, co-edited by Ronald Hes and John Borking). For an early overview of PETs, *see* Herbert Burket, *Privacy-Enhancing Technologies: Typology, Critique, Vision, in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 125 (Philip E. Agre & Marc Rotenberg eds.) (1998) (defining PETs as "[seeking] to eliminate the use of personal data altogether or to give direct control over revelation of personal information to the person concerned").

determine whether a website's practices are consistent with their own, with the goal of making users better equipped to make informed choices.[196]

These initiatives all tend to follow a similar pattern. Sponsors launch the new PET with overly enthusiastic claims about its benefits, while at least a few privacy advocates denounce the PET as a subterfuge devised by industry mainly for the purpose of blocking new privacy legislation. For its part, the FTC may offer qualified support of the new PET in testimony, staff reports, speeches, or industry consultations, but refrains from taking a stance on any disputed regulatory issues. P3P is a paradigmatic case. Although W3C presented P3P as part of a larger, more comprehensive set of technical and legal solutions and never contended that it solved all privacy concerns on the Web,[197] Microsoft, AOL and Netscape behaved as if it largely obviated the need for an omnibus privacy law.[198] Meanwhile, EPIC and others condemned P3P harshly on numerous grounds.[199] Finally, while the FTC supported P3P to the extent of testifying that a new privacy law might interfere with P3P's broad adoption by imposing incompatible notice requirements, the Commission never sought to resolve any of the legal issues concerning P3P that may have slowed its deployment.[200]

Project XL offers an alternative approach to this stalemate. As noted previously, experimental XL projects require a firm, trade

---

[196] *See* World Wide Web Consortium, The Platform for Privacy Preferences 1.1 (P3P1.1) Specification, http://www.w3.org/TR/P3P11/ (last visited July 12, 2011).

[197] *See* World Wide Web Consortium, P3P and Privacy FAQ, http://www.w3.org/P3P/p3pfaq.html#solve (last visited July 12, 2011).

[198] *See, e.g.*, Glenn R. Simpson, *The Battle Over Web Privacy: As Congress Mulls New Laws, Microsoft Pushes a System That's Tied to Its Browser*, WALL ST. J., March 21, 2001, at B1.

[199] *See, e.g.*, Electronic Privacy Information Center & Junkbusters Corp., Pretty Poor Privacy: An Assessment of P3P and Internet Privacy (2000), *available at* http://www.epic.org/reports/prettypoorprivacy.html (last visited Mar. 14, 2011).

[200] *See* S. 2201, *Online Personal Privacy Act, Hearing on S. 2201 Before the Comm. on Commerce, Science and Transportation*, 107th Cong. 11 (2002) (statement of Tim Muris, Chairman, Fed. Trade Commission), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_senate_hearings&docid=f:91368.pdf. The worrisome legal issues included the extent to which P3P policies were legally binding and/or fully discharged legal obligations under applicable notice and choice requirements, and how websites should deal with limitations of the P3P vocabulary, which made it difficult to express company privacy policies in P3P code.

association, or standards organization to submit to the FTC a proposal describing their new initiative in detail, including how it does a better job of protecting consumer privacy, whether it has the support of various stakeholders, and what changes, if any, in existing (or new) regulations might be required. Thus, innovative ideas developed within a Project XL framework not only could achieve greater regulatory certainty for their sponsors and early adopters, but might also win the support of advocacy groups if they were consulted at the outset and given an opportunity to review a PET's design and implementation before it was set in stone. Ideally, all of the stakeholders would discuss whether the new approach achieves a high enough standard of privacy protection to justify regulatory relief, such as the FTC establishing clear guidelines for ensuring that P3P policies harmonize with written privacy statements while treating them as enforceable promises.[201] Certainly, a high profile project like P3P would have benefited from a more collaborative process in which all affected parties and the regulators worked together to embrace P3P's strong points rather than squabbling over its weak points.

In addition to experimenting with PETs that help implement FIPPs, the XL process also might be appropriate for exploring new approaches to privacy protection that refocus or even supplant FIPPs. For example, Fred Cate has suggested a new approach that emphasizes tangible harms. Cate argues that despite their lofty goals, FIPPs fail in practice by "maximizing consumer choice" rather than "protecting privacy while permitting data flows."[202] He has outlined a revised version of FIPPs with new principles emphasizing the prevention of harm, the maximization of individual and public benefits through the balancing of the value of accessible personal information and information privacy, and more consistent privacy protection across all types of data, settings, and jurisdictions. In shifting attention from notice and choice to tangible harms, Cate's proposed principles also emphasize substantive rather than procedural protections.[203]

---

[201] *See* William McGiveran, Note, *Programmed Privacy Promises: P3P and Web Privacy Law*, 76 N.Y.U. L. REV. 1812 (2001) (recommending that lawmakers combine P3P code with market forces and a legal rationale based on enforcement of promises).

[202] *See* Fred *H. Cate, The Failure of Fair Information Practice Principles, in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 369 (Jane K. Winn ed., 2006).

[203] Similarly, a group of MIT researchers argue that a privacy regime premised on controlling and preventing access to information no longer works given the ease of sharing data and the large-scale aggregation and searching of data across multiple sources. Their new approach is based on transparency and accountability of data *use*, and their work

Of course, not every privacy-enhancing initiative needs or deserves an XL project. In the environmental arena, the benefits of Project XL are reasonably clear: regulatory flexibility, reduced compliance costs, and greater certainty regarding the regulatory implications of using new technologies or more integrated approaches. But privacy law is not nearly as hard and fast as environmental regulation, nor is FTC enforcement as extensive or costly as the EPA's civil, clean-up, and criminal enforcement programs. As a result, only a handful of highly regulated privacy leaders are likely to pursue a privacy-related XL project given the burdens of doing so and the high standards that the stakeholders and the FTC would require to obtain any guarantee of regulatory relief.[204] Nor would an FTC version of Project XL necessarily overcome the flaws in the original program, such as the need for baseline requirements, better guidance regarding stakeholder participation, and (absent a statute) a lack of clear legal authority. But the FTC could mitigate these problems by learning from the EPA experience and following Hirsch's advice: select a few meritorious projects with clear goals, devise an appropriate stakeholder process, and postpone any broader policy decisions until the experimental projects have been thoroughly scrutinized.

B. NEGOTIATED RULEMAKING AND ONLINE BEHAVIORAL ADVERTISING

Should the FTC engage in negotiated rulemaking when issuing rules governing the online collection of personal information? Before considering the potential advantages of this approach, a brief discussion of the FTC's rulemaking authority is needed, given that it stems from two quite different sources. The first is Section 18 of the FTC Act, under which the Commission has *limited* authority to prescribe rules defining "unfair or deceptive acts or practices in or

---

describes a new technical architecture for promoting informational accountability. *See* Daniel J. Weitzner, et al., *Information Accountability*, 51 COMM. OF THE ASS'N FOR COMPUTING MACHINERY 82, 86 (2008) (arguing that "privacy is protected not by limiting the collection of data, but by placing strict rules on how the data may be used"). Additionally, the Business Forum for Consumer Privacy has proposed a new "use-and-obligations" model for implementing FIPPs based on Cate's work. *See* BUS. FORUM FOR CONSUMER PRIVACY, *A USE AND OBLIGATIONS APPROACH TO PROTECTING PRIVACY: A DISCUSSION DOCUMENT (2009), available at* http://www.ftc.gov/os/comments/privacyroundtable/544506-00058.pdf.

[204] This point was suggested to me by Lisa Sotto.

affecting commerce."[205] The second would be a new privacy law authorizing the FTC to issue implementing regulations.

Before commencing rulemaking under Section 18, the Commission must jump over the high hurdles set by Congress in 1980 in response to perceived abuses of the agency's rulemaking authority. These requirements include advance rulemaking notice to Congress and the public, public hearings at which interested parties have limited rights of cross-examination, and a statement of basis and purpose addressing both the prevalence of the acts or practices specified by the rule and its economic effect.[206]

On the other hand, when Congress grants the FTC rulemaking authority to address a more narrowly focused problem under a specific statute, the Commission may, at its discretion, rely on the notice and comment rulemaking procedures followed by most federal agencies or on negotiated rulemaking. In the past, the Commission has followed APA procedures in issuing rules regulating children's privacy,[207] financial privacy,[208] and the standards for commercial

---

[205] *See* 15 U.S.C. § 57a(a)(2).

[206] *See* 15 U.S.C. § 57a(b)(1)-(2). *See generally* JULIAN O. VON KALINOWSKI ET AL., ANTITRUST LAWS AND TRADE REGULATION § 5.14 (1997). The FTC's limited rulemaking authority under § 18 merits some further explanation, although readers mainly interested in negotiated rulemaking may safely skip this footnote. Due to the burdensome and time-consuming procedures imposed by § 18, the FTC often prefers to rely on strategic enforcement actions to achieve its regulatory goals. This seems consistent with published statements of how the Commission views its options for regulating privacy practices. For example, in a July 14, 2000 letter to the EC explaining the agency's jurisdiction over such practices, former Chairman Pitofsky indicated that while § 5 clearly provides a legal basis for enforcement actions against firms that misrepresent their privacy practices (deceptive practices) or that fail to secure their customers' personal information (unfair practices), "it currently may not be within the FTC's power to broadly require that entities collecting information on the Internet adhere to a privacy policy or to any particular privacy policy." *See* Issuance of Safe Harbor Principles, *supra* note 137, at 45,883-85. More recent statements by Leibowitz and Vladeck suggest that the Commission is reconsidering this policy as a result of dissatisfaction with a consumer privacy strategy based primarily on enforcement and self-regulation. *See supra* notes 41-43 and accompanying text. If Congress does not enact new substantive privacy law, it will be interesting to see if the Commission rethinks the appropriateness of using § 18 to promulgate a rule requiring adherence to FIPPs. Although an early draft of the recently enacted financial reform bill included a provision amending § 57a(b) of the FTC Act to allow the Commission to promulgate rules defining unfair or deceptive practices using conventional rulemaking procedures under the APA, without having to observe any additional procedural safeguards, this amendment was dropped from the final version of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2009. *See* Wall Street Reform and Consumer Protection Act of 2009, H.R. 4173, 111th Cong. § 4901 (2009).

[207] *See* COPPA, 15 U.S.C. § 6503(b)(1).

email marketing.[209] But nothing prevents it from initiating a negotiated rulemaking in the future if it were to modify an existing rule under COPPA, GLBA or CAN-SPAM; or, in the alternative, if Congress were to enact new, substantive privacy legislation and the statute specifically authorized the Commission to engage in APA rulemaking.

With these preliminaries taken care of, if Congress passes a bill along the lines suggested by Rep. Boucher, the FTC *should* rely on negotiated rulemaking to address the privacy concerns raised by behavioral targeting. The Boucher draft already includes a safe harbor provision in Section 3(e), which exempts advertising networks that track online behavior from having to obtain explicit, opt-in consent provided that they allow consumers to view and modify, or opt out of entirely, the profile maintained about them for advertising purposes, and directs the FTC to promulgate a rule implementing this provision.[210] As discussed previously, negotiated rulemaking is most beneficial when the underlying rule requires information sharing between the regulators, the regulated industry, and other affected parties, and when the parties believe they have something to gain from working together and achieving a compromise.[211] Arguably, these conditions would be met if the FTC formed a negotiated rulemaking committee to tackle a safe harbor rule addressing behavioral targeting.

A negotiated rulemaking for behavioral targeting may strike the reader as quixotic. After all, industry's bottom line is to maintain the free flow of information including personal data needed for ad targeting, which in turn increases advertising revenues. Hence, it strongly favors an opt-out regime backed by accountability measures such as compliance reviews conducted by trade associations. Advocates, on the other hand, seek more meaningful protection from intrusive profiling. Hence, they demand legislative solutions based on opt-in choice, a broader definition of PII, very short data retention periods, and external audits. These differences are deep-seated and perhaps ideological, and thus not easily overcome. Yet there is reason to believe that all of the affected parties—the regulated industry, the

---

[208] *See* GLBA, 15 U.S.C. §§ 6801, 6804, 6805(b)(2).

[209] *See* Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003, 15 U.S.C. § 7711.

[210] *See* Staff of Richard Boucher, *supra* note 14.

[211] *See supra* notes 69–72 and accompanying text.

advocates representing the public interest, and the regulators—might be highly motivated to engage in face-to-face negotiations and would benefit from the information sharing that inevitably occurs in this setting.

As to motivation, industry should first recognize that if Congress enacts a new privacy law, it is very likely to regulate behavioral targeting, while if Congress fails to act, Leibowitz and Vladeck are very likely to reject further self-regulation as inadequate and instead pursue a far more aggressive enforcement strategy or even a new rulemaking directed at behavioral targeting practices (assuming they determine that the FTC has sufficient rulemaking authority under Section 18).[212] Second, advocates should realize that they face an uphill battle in persuading Congress that new privacy legislation would have no negative economic impacts on the online advertising revenues that currently subsidize free online content and services, or that a drop in these revenues won't result in higher costs for consumers. Third, the FTC is not yet locked into any one approach. To the contrary, when Leibowitz was recently asked what people should expect from the FTC's roundtable series on privacy and where the agency was headed, he answered, "I can honestly say: we don't know. Our minds are open."[213]

Finally, as to information sharing, the negotiated rulemaking process by its very nature encourages more credible transmission of information among the parties. To begin with, the network advertising industry undoubtedly possesses greater expertise and insight into the complex technology and evolving business models underlying OBA than either privacy advocates or FTC staff. In the past, this information has been shared or elicited mostly through one-sided communications—unilateral codes of conduct, complaints filed with the FTC, or charges and countercharges at public forums. In a

---

[212] *See supra* note 206.

[213] *See* JON LEIBOWITZ, CHAIRMAN, FED. TRADE COMMISSION, INTRODUCTORY REMARKS AT THE FTC'S EXPLORING PRIVACY-A ROUNDTABLE SERIES (Dec. 7, 2009), *available at* http://www.ftc.gov/speeches/leibowitz/091207privacyremarks.pdf; *see also* Vladeck Interview, *supra* note 43 (when asked what he meant by clearer notice and consent, Vladeck stated, "I don't want to suggest that we've prejudged anything. I think the key is transparency across the board .... I don't know whether we'd gravitate toward a universal opt-in"). On December 1, 2010, the FTC issued its report on the roundtables; *see* FED. TRADE COMMISSION (BUREAU OF CONSUMER PROTECTION), A PRELIMINARY FTC STAFF REPORT ON PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf. FTC [hereinafter FTC Proposed Framework].

negotiated rulemaking process, however, the logic of Coasian bargaining prevails. In other words, each party seeks to "maximize its share of the gains produced by departure from standard requirements" and this requires that parties "educate each other, pool knowledge, and cooperate in problem solving."[214] In short, when both sides engage in explicit bargaining over priorities and tradeoffs, they are far more likely to achieve a satisfactory compromise than by relying on the indirect communications that characterize conventional notice and comment rulemaking.

C. STATUTORY SAFE HARBORS REVISITED

The previous section examined the potential use of negotiated rulemaking in the event that Congress enacted a new law that included a safe harbor exemption for firms that collect and use data for OBA purposes, provided they follow certain specified practices. This section offers a much broader look at how Congress might integrate the covenanting approach into any new privacy legislation by including a revamped safe harbor provision. Assume for the sake of argument that Congress enacts privacy legislation requiring websites that collect information from Internet users to follow default requirements based on FIPPs, unless they participate in an approved safe harbor modeled on §6503 of COPPA. A modest approach to redesigning this safe harbor might be to add several new elements based on the Dutch and Australian privacy codes discussed above. For example, Congress might grant the FTC broad discretion to approve self-regulatory guidelines for different industry sectors so long as (1) the organization seeking approval is sufficiently representative of the sector; (2) industry members consult with other interested parties, including privacy and consumer advocacy groups, and/or engage in direct negotiations with them; (3) industry clearly justifies any derogation from FIPPs; (4) the Commission reviews industry guidelines under a notice and comment process before final approval; and (5) approved guidelines bind only those companies that chose to participate.[215]

---

[214] *See* Freeman & Langbein, *supra* note 70, at 69. For a very similar point, *see* Morriss, *supra* note 94, at 201 (observing that "agencies may need the negotiation process to allow one set of interests to make credible commitments or disclosures to another set of interests that enable the regulation to be recognized as a Pareto improvement").

[215] *Compare* the Rush bill, *supra* note 15, at §§ 401–404. The Choice Program enables firms to qualify for certain exemptions provided the program meets the following five requirements: (1) a "universal" opt-out mechanism and preference management tool that

Of course, this brief description raises more questions than it answers. Which trade associations should FTC work with, especially if there are competing organizations with overlapping membership? How are firms and NGOs selected and how many should participate? May a large firm that has several different divisions and belongs to several trade groups participate in multiple negotiations and assume obligations under multiple codes? What about smaller firms that may not belong to any trade association? How do they ensure proper representation in negotiations that might affect them?[216] If NGOs lack the necessary resources to staff negotiation sessions (which seems very likely), should government or industry help fund their participation? Should there be a specified period for completion of negotiations and/or submission of a draft code? Should negotiations occur in open sessions or behind closed doors, with only stakeholders in attendance? If a firm or NGO walks out on the negotiating process, does the FTC retain discretion to commence a notice and comment process for a code that it nevertheless considers satisfactory? The negotiated rulemaking process answers many of these questions, so perhaps Congress should encourage its use as the principal (but not exclusive) method of approving proposed safe harbor programs under a new privacy law.

For a new safe harbor program to have much likelihood of success, Congress would also need to ensure that industry did not view privacy codes as requiring a high expenditure of resources while offering too few tangible benefits (as seems to be the case with both COPPA and the Australian privacy codes). This requires not only well-designed legislation but far more deliberate attention than existing schemes give to developing the right combination of incentives. As to the design issue, Congress could define specific standards as a default, but then allow the FTC to negotiate tailored requirements with industry trade groups; adherence to these requirements would then substitute

---

applies an individual's choices to all firms participating in the program; (2) guidelines and procedures that offer equivalent or greater protections than those required in Title I (transparency, notice and individual choice) and Title II (accuracy, access and dispute resolution); (3) approval procedures for participating firms; (4) procedures for periodic self-assessment and random compliance testing; and (5) consequences for failure to comply with program requirements. Qualifying firms are not subject to the express affirmative consent requirements under § 104(a), the access requirement under § 202(b), or liability in a private right of action brought under § 604.

[216] Arguably, a well-organized industry with broad trade association membership is a pre-condition for the sector-based covenanting approach. However, firms that do not belong to a trade association should be permitted to adapt the model rules of any trade association in their industry sector. *See* AYRES & BRAITHWAITE, *supra* note 46, at 121.

for compliance with the default standards. Those firms that did not sign up for a code of conduct still would have to comply with the default requirements, thereby addressing the free-rider problem. But the FTC would need to pay more than lip service to allowing flexibility in the development of industry guidelines and to taking into account industry-specific concerns and technological developments.

As to incentives, Congress should use both sticks and carrots.[217] In the environmental setting, sticks typically include a threat of stricter regulations or the imposition of higher pollution fees. Carrots might take the form of more flexible regulations, recognition of better performance by the government, and cost-savings such as exemptions from mandatory reporting, or easier and quicker permitting. Firms that demonstrate high performance avoid these sticks and/or enjoy these carrots. What sticks and carrots might be devised to enhance a new privacy safe harbor, given that the COPPA safe harbor relied primarily on deemed compliance and a largely empty promise of regulatory flexibility? Over the years, many advocacy groups and privacy scholars have favored a private right of action and liquidated damages as enforcement mechanisms in any new privacy legislation. Not surprisingly, industry has argued that such remedies are both unnecessary and ineffective. This suggests that a tiered liability system might make an excellent stick. Under this approach, new privacy legislation would allow civil actions and liquidated damage awards against firms that did not participate in an approved safe harbor program. In sharp contrast, compliance with approved self-regulatory guidelines would not only serve as a safe harbor in any enforcement action, but also protect program participants from civil lawsuits and monetary penalties.[218]

While tiered liability is a novel concept in privacy law, it is worth pointing out that *Black's Law Dictionary* defines safe harbor as a "provision (as in a statute or regulation) that affords protection from liability or penalty"[219] and that such safe harbors are extremely common statutory devices. For example, Section 102 of the Private Securities Litigation Reform Act (PLSRA)[220] provides a safe harbor for projections of future economic performance if they meet a (much

---

[217] *See* FIORINO, *supra* note 66, at 124.

[218] *See supra* note 15, at § 604.

[219] *See* BLACK'S LAW DICTIONARY 1140 (Abridged 9th ed. 2005) (defining "safe harbor").

[220] 15 U.S.C. § 78-u5 (1995).

litigated) standard of good faith. Similarly, the safe harbor under Section 512 of the Digital Millennium Copyright Act[221] seeks to immunize Internet service providers from copyright liability if they adhere to certain guidelines designed to protect the rights of authors. In contrast, the Section 230 safe harbor in the Communications Decency Act[222] provides complete immunity from liability for providers and users of an "interactive computer service" who publish information provided by others.

Not all safe harbors shield participants from liability, however. Some safe harbor programs take the form of exemptions from statutory requirements. For example, Title VII of the Civil Rights Act of 1964 does not apply to private sector employers with fourteen or fewer employees.[223] And the California security breach notification law only imposes its notice requirement on "unencrypted data."[224] Finally, some safe harbors permit regulated entities to engage in desired behavior provided that they meet certain conditions. For example, as noted above, the SHA treats U.S. firms that self-certify as providing an adequate level of privacy protection and thereby enables transfers of E.U. data to the U.S. Under the COPPA safe harbor program, participating firms are deemed to be in compliance with all statutory requirements.[225] Similarly, financial institutions regulated by the GLBA that use the model privacy form described in Appendix A to the Privacy Rule are deemed to be in compliance with the rule's notice requirements.[226]

As to carrots, they might include official government recognition of superior performance by top-tier performers in safe harbor programs (while non-participating firms would be ineligible for such recognition), as well as certain purchase preferences. The federal government gives a preference to Energy Star products. Why not also give a preference to email, search, or other internet technologies or services acquired from safe harbor firms?

---

[221] 17 U.S.C. § 512 (1998).

[222] 47 U.S.C. § 230(c) (2000).

[223] 42 U.S.C. § 2000(e) (1964).

[224] *See* CAL. CIV. CODE. § 1798.82.

[225] *See supra* note 154.

[226] *See* 16 C.F.R. § 313.2 (2009).

The last few paragraphs describe a proposed regulatory strategy in which federal privacy law would formally recognize differences in performance by treating safe harbor participants differently from non-participants. This is true of all safe harbor schemes. Their function is to shield or reward regulated firms if they engage in desirable behavior as defined by statute. A few safe harbor provisions, like the small business exemption under Title VII, leave no doubt as to whether a regulated firm qualifies for differential treatment. But this is unusual. More often than not, the conditions for eligibility are sufficiently complex that litigation is required to sort them out, and even then the courts often disagree.[227]

What, then, are the privacy practices that industry must follow to be eligible for safe harbor treatment? Before addressing this key issue, a brief summary of the argument so far is in order. Any privacy legislation that Congress is likely to enact is bound to address the core FIPPs: notice, consent, access, data security, data minimization, data integrity, accountability, and enforcement. Under such a statute, firms would be obliged to provide notice via a privacy statement, offer relevant consent choices depending on their data collection and use practices, provide reasonable access to personal data and a limited ability to correct or amend that data, and implement reasonable security practices. Mere compliance with these legal requirements *should not* entitle a firm to safe harbor treatment. Rather, one of the purposes of second-generation strategies like those described in the previous section is to distinguish good performers from bad performers, and to treat them accordingly. This means reserving safe harbor benefits (both availability of carrots and avoidance of sticks) for firms that sign up for a sectoral agreement that goes *beyond* mere

---

[227] For example, courts have disagreed on whether the PLSRA safe harbor immunizes forward-looking statements that are accompanied by "meaningful cautionary statements" if the statements were false and made with actual knowledge of their falsity. *Compare* Freeland v. Iridium World Comm., 545 F. Supp. 2d 59 (D.D.C. 2008) *with* Beaver County Ret. Bd. v. LCA-Vision Inc., No. 1:07-CV-750, 2009 WL 806714 (S.D. Ohio Mar. 25, 2009). For an example of denying safe harbor protection under DMCA § 512 to firms that use peer-to-peer networking systems to facilitate file sharing over the Internet, *see* A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001); *see also* In re Aimster Copyright Litigation, 35 252 F. Supp. 2d 634, 648 (N.D. Ill. 2002), *aff'd*, 334 F.3d 643 (7th Cir. 2003). And for an example of denying § 230 immunity to an online roommate matching service that was potentially liable under the Fair Housing Act for requiring members to answer questions that potentially enabled other members to discriminate for or against them, *see* Fair Housing Council of San Fernando Valley v. Roommate.com, LLC, 521 F.3d 1157 (9th Cir. 2008) (en banc).

compliance as determined by suitable performance measures.[228] Obviously, this requires reliable performance measures, such as (in the environmental field) exceeding targeted goals for reducing pollution or emissions.[229] Arguably, privacy performance is harder to measure than air or water quality given not only "the vagueness and contestability" of the meaning of privacy, but also the lack of any meaningful quantitative indicators.[230] At the very least, the science of measuring privacy performance is in the early stages of development. What steps firms should take to achieve higher levels of privacy protection for consumers is a very large and complex topic, and well beyond the scope of this paper. Suffice to say that these steps are likely to include three components: data governance, privacy methodologies, and best practices.[231]

---

[228] *See* FIORINO, *supra* note 66, at 200–01 (describing how agencies might incorporate performance tiers into regulations by defining criteria for differentiating among firms and deciding how top performers should be treated differently).

[229] *See supra* note 67.

[230] *See* COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 242 (2006) (noting several difficulties in evaluating the quality of data protection).

[231] For a preliminary description of a holistic approach to privacy protection incorporating all three subcomponents, a good source is a Discussion Document prepared for the U.K. Information Commissioner's Office. *See* CONSUMER FOCUS, THE BUSINESS CASE FOR INVESTING IN PROACTIVE PRIVACY PROTECTION (2009), *available at* http://www.consumerfocus.org.uk/assets/1/files/2009/11/TheBusinessCaseforInvestinginProactivePrivacyProtection.pdf. For more on data governance, *see, e.g.*, EUR. COMMISSION, OPINION 3/2010 ON THE PRINCIPLE OF ACCOUNTABILITY, *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf; *see also* various materials from the Center for Information Policy Leadership's project on Accountability-Based Privacy Governance, http://www.hunton.com/Resources/Sites/general.aspx?id=965 (last visited Feb. 3, 2011). Privacy methodologies are sometimes discussed under the rubric of Privacy by Design. *See, e.g.*, EUR. COMMISSION, A DIGITAL AGENDA FOR EUROPE (2010), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:HTML (describing "the principle of privacy by design" in terms of embedding privacy and data protection throughout the entire lifecycles of technologies, from the early design stage to their deployment, use and ultimate disposal); *see also* FTC Proposed Framework, *supra* note 213 at 44–52 (identifying privacy by design as one of three major recommendations resulting from the roundtables). In addition, Joint Technical Committee 1 of the International Standards Organization (ISO) is examining the relation of privacy to information technology. In particular, Subcommittee 27 (SC 27), IT Security Techniques, is working on several projects, including its "Privacy Framework," "Privacy Reference Architecture," and "Proposal on a Privacy Capability Assessment Model." *See* IT Security Techniques,

Much work remains to be done on the necessary and sufficient criteria for improving privacy performance, and on how exactly they might be translated into performance measures for purposes of safe harbor eligibility. Two points are clear, however. First, government should rely principally on the private sector, academia, and international standards bodies for further development of the holistic approach described above. Second, government should not attempt to define performance measures. Rather, it should support existing efforts to develop such measures by funding academic research; encouraging U.S. trade associations and firms to participate in international standards efforts; and, as these standards mature, promoting market demand through purchasing criteria, giving preferred regulatory treatment to firms that meet these emerging requirements, or expressly adopting privately generated standards in public regulation.[232]

V. CONCLUSION AND RECOMMENDATIONS

Whatever its shortcomings, and despite its many critics, self-regulation is a recurrent theme in the U.S. approach to online privacy, and perhaps a permanent part of the regulatory landscape in America. This Article's goal has been to consider new strategies for overcoming observed weaknesses in self-regulatory privacy programs. It began by examining the FTC's intermittent embrace of self-regulation, and found that the Commission's most recent foray into self-regulatory guidelines for online behavioral advertising is not very different from earlier efforts, which ended in frustration and a call for legislation. It argued that any attempt to treat this privacy debate exclusively in terms of voluntary codes versus prescriptive regulation rests on a false dichotomy that needs to be abandoned in favor of more innovative regulatory solutions.

---

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306&development=on (last visited Mar. 14, 2011).

[232] Once again environmental law provides insights into these policy instruments. *See, e.g.*, Hirsch, *supra* note 66, at 60–63 (discussing Environmental Management Systems (EMSs) as a model for using organizational practices and procedures to improve privacy); *see also* FIORINO, *supra* note 66, at 144–49 (describing the EPA's National Environmental Performance Track, which gives special treatment to firms meeting four criteria: (1) sustained compliance with environmental law, (2) use of an EMS, (3) public outreach, and (4) committing to continuous improvement in environmental performance); Errol E. Meidinger, *Environmental Certification Programs and U.S. Environmental Law: Closer Than You May Think*, 31 ENVTL. L. REP. 10, 162 (2001) (describing environmental certification programs and how they are incorporated into legal systems).

Next, it identified different types of self-regulation and then examined the co-regulatory approach based on covenants, using Coasian bargaining principles to explain why environmental covenants such as Project XL and negotiated rulemaking were likely to achieve a superior outcome as compared to conventional rulemaking. It also developed a normative framework consisting in six factors (efficiency, transparency and openness, completeness, addressing free rider problems, oversight and enforcement, and use of second-generation strategies), and applied them to four case studies. This exercise demonstrated that self-regulation, undergirded by law (as is the case in negotiated agreements such as Project XL and regulatory negotiations, and as is the case in a *statutory* safe harbor) is a more effective and efficient instrument than either voluntary codes (which, lacking government oversight and enforcement, are often too lax) or prescriptive regulation (which, lacking industry input and expertise, may be too inflexible and inefficient). In a nutshell, well-designed safe harbors enable policy makers to imagine new forms of self-regulation that "build on its strengths . . . while compensating for its weaknesses."[233] This embrace of statutory safe harbors and a discussion of privacy covenants as a transitional regulatory instrument led to a discussion of three specific proposals for improving privacy self-regulation. Rather than summarizing these proposals as described in Part IV, this Article concludes with a set of specific recommendations to Congress as it considers privacy legislation in the coming years.

The first recommendation is that Congress includes a provision in any new bill permitting experimental privacy XL projects. Specifically, the provision should authorize the FTC to negotiate covenants with firms modifying or relaxing fair information practices in exchange for enforceable promises to achieve better results in one or more areas covered by the legislation (such as transparency, individual participation, purpose specifications, data minimization, use limitations, data quality and integrity, security, or accountability and auditing) using new approaches to data governance, innovative technologies, or other best practices. Allowing the FTC and the relevant stakeholders to identify and experiment with worthy projects within the XL framework is likely to yield better results than if Congress itself selects interesting ideas and obliges the FTC to report on them in a fixed timeframe.[234]

---

[233] *See* Gunningham & Rees, *supra* note 6, at 389.

[234] *See, e.g.*, CAN-SPAM Act, 15 U.S.C. § 7708 (requiring the FTC to report on the feasibility of a Do-Not-Email Registry); *see also* 15 U.S.C. § 7710 (requiring the FTC to

The second recommendation is that any new law based on FIPPs should include a safe harbor program echoing the COPPA safe harbor to the extent that it encourages groups to submit self-regulatory guidelines and, if approved by the FTC, that it treats compliance with these guidelines as deemed compliance with statutory requirements. The FTC should be granted APA rulemaking powers to implement necessary rules, including a safe harbor rule. Congress should also consider whether to mandate negotiated rulemaking for a behavioral advertising safe harbor. In any case, the FTC should give serious thought to using the negotiated rulemaking process in developing a safe harbor program or approving specific guidelines. Alternatively, the safe harbor rule should require applicants to demonstrate that they have engaged in stakeholder consultation by describing, for example, who is affected by the proposed safe harbor program, what efforts the applicant has taken to consult with affected groups (including the period of time allowed for such consultations), any changes to the proposed safe harbor guidelines resulting from these consultations, and a summary of any issues that remain unresolved and why.[235]

In addition, the COPPA-style safe harbor program should be overhauled to reflect second-generation strategies. Specifically, the statute should articulate default requirements but allow the FTC more discretion in determining whether proposed industry guidelines achieve desired outcomes, without firms having to match detailed regulatory requirements on a point-by-point basis. Additionally, the enforcement provision should include new incentives such as tiered liability and lighter regulatory burdens for firms that qualify for safe harbor treatment.[236] Finally, because performance measures for privacy remain an underdeveloped area with scant literature describing these measures or their usefulness in predicting superior performance, the FTC should at the very least be encouraged to

---

report on a "bounty" system for rewarding members of the public who help catch spammers and the use of "ADV" labeling in subject lines to help identify commercial emails).

[235] *See Legislative Hearing Examining H.R. 5777, the BEST PRACTICES Act, and the Boucher-Stearns Discussion Draft Before the Subcommittee on Commerce, Trade, and Consumer Protection of the House Comm. on Energy and Commerce*, 111th Cong. (2010) (testimony of Ira Rubinstein), *available at* http://republicans.energycommerce.house.gov/Media/file/Hearings/CTCP/072210_CTCP_Best_Practices/Rubinstein.Testimony.pdf.

[236] The Choice Program in the recently introduced Rush bill adopts a very similar approach. *See* Best Practices Act, *supra* note 15 at § 401(3).

support non-governmental efforts to develop appropriate measures of privacy performance.